

# HP Integrated Lights-Out User Guide



June 2003 (Fourth Edition)  
Part Number 238882-004

© 2003 Hewlett-Packard Development Company, L.P.

Microsoft®, Windows®, MS-DOS® and Windows NT® are U.S. registered trademarks of Microsoft Corporation.

Java™ is a U.S. trademark of Sun Microsystems, Inc.

Hewlett-Packard Company shall not be liable for technical or editorial errors or omissions contained herein. The information in this document is provided “as is” without warranty of any kind and is subject to change without notice. The warranties for HP products are set forth in the express limited warranty statements accompanying such products. Nothing herein should be construed as constituting an additional warranty.

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

June 2003 (Fourth Edition)

Part Number 238882-004

### **Audience Assumptions**

This guide is for the person who installs, administers, and troubleshoots servers. HP assumes you are qualified in the servicing of computer equipment and trained in recognizing hazards in products with hazardous energy levels.

# Contents

## Configuring Integrated Lights-Out 13

iLO Configuration Options .....	13
iLO RBSU .....	14
Browser-Based Setup.....	15
Optimizing Performance for Graphical Remote Console .....	16
Recommended Client Settings.....	16
Recommended Server Settings .....	17
Enabling iLO Advanced Functionality .....	18
Installing iLO Device Drivers .....	19
Microsoft Windows NT, Windows 2000, and Windows Server 2003 Driver Support.....	20
Novell NetWare Server Driver Support.....	21
Red Hat Linux and SuSE Linux Server Driver Support .....	22

## Using Integrated Lights-Out 25

Supported Server Operating System Software.....	25
Supported Browsers .....	26
Single and Dual Cursor Modes for Graphical Remote Console.....	27
Remote Console (Dual Cursor).....	27
Remote Console (Single Cursor) .....	27
Common Usage Model .....	28
Connection Overview .....	29
Corporate Network Connection .....	29
Integrated Lights-Out Network Connection .....	30
Operational Overview .....	30
Accessing iLO for the First Time.....	35
Progressive Delays for Failed Browser Login Attempts.....	39
Help .....	40
System Status .....	40
Status Summary.....	40
iLO Status .....	40
Server Status.....	41
iLO Event Log .....	42
Integrated Management Log.....	43
Server and iLO Diagnostics.....	43
Remote Console .....	45
Remote Console Information Option.....	46
Remote Console Option.....	46

Remote Console (Dual Cursor) Mode .....	49
Virtual Devices .....	50
Virtual Power Button .....	51
Virtual Media .....	53
Using iLO Virtual Media Devices .....	55
Virtual Serial Port .....	61
Virtual Indicators .....	62
Administration .....	63
User Administration .....	63
Network Settings .....	65
Global Settings .....	68
SNMP/Insight Manager Settings .....	72
Upgrade iLO Firmware .....	74
Licensing .....	76
Certificate Administration .....	76
Directory Settings .....	77
ProLiant BL p-Class .....	77
Rack Settings .....	77
Rack Topology .....	80
Server Blade Management Module .....	81
Power Management Module .....	81
Redundant Power Management Module .....	82
iLO Control of ProLiant BL p-Class Server LEDs .....	82
Telnet Support .....	83

---

**Insight Manager 7 Integration 85**

---

Functional Overview .....	85
Identification and Association .....	85
Status .....	86
Queries .....	86
Links .....	86
Alerts .....	87
Port Matching .....	87
Configuring Identification of iLO .....	88
Integrating iLO with Insight Manager 7 .....	89
Receiving SNMP Alerts in Insight Manager 7 .....	90
Reviewing iLO Advanced Pack License Information in Insight Manager 7 .....	91
ProLiant BL p-Class Rack Visualization .....	91

---

**Security for Integrated Lights-Out 93**

---

General Security Guidelines .....	93
Encryption .....	93
iLO Security Override Switch Administration .....	93
User Accounts .....	95

Privileges .....	95
Global Security Settings .....	95
Login Security .....	96
Passwords.....	96
Certificates .....	97

---

## Directory Services 99

Introduction to Directory Services .....	99
Schema Documentation .....	99
Directory Services Support .....	100
Required Software.....	101
Schema Installer.....	101
Schema Preview .....	101
Setup.....	102
Results .....	104
Management Snap-In Installer .....	104
Directory Services for Active Directory .....	105
Active Directory Installation Prerequisites .....	105
Directory Services Preparation for Active Directory.....	105
Snap-in Installation and Initialization for Active Directory .....	107
Directory Services Objects for Active Directory.....	113
Active Directory Lights-Out Management .....	121
Directory Services for eDirectory .....	122
eDirectory Installation Prerequisites.....	122
Snap-in Installation and Initialization for eDirectory .....	123
Directory Services Objects for eDirectory.....	128
Role Restrictions.....	131
Lights-Out Management.....	134
Configuring Directory Settings.....	135
Directory Tests .....	137
User Login to iLO .....	138

---

## Group Administration and Integrated Lights-Out Scripting 141

Features of the Lights-Out Configuration Utility .....	141
Group Administration Using the Lights-Out Configuration Utility and Insight Manager 7 .....	142
Lights-Out Configuration Utility .....	142
Query Definition in Insight Manager 7.....	143
Application Launch Using Insight Manager 7 .....	144
Batch Processing Using the Lights-Out Configuration Utility.....	145
Lights-Out Configuration Utility Parameters .....	146

---

## Lights-Out DOS Utility 149

Overview of the Lights-Out DOS Utility .....	149
--	-----

CPQLODOS General Guidelines.....	150
Command Line Arguments.....	150
CPQLODOS .....	152
CPQLODOS Parameter.....	152
CPQLODOS Runtime Error.....	152
MOD_NETWORK_SETTINGS.....	152
MOD_NETWORK_SETTINGS Parameters.....	153
MOD_DIR_CONFIG.....	155
MOD_DIR_CONFIG Parameters.....	156
ADD_USER.....	157
ADD_USER Parameters.....	157

## Remote Insight Command Language 159

---

Overview of the Remote Insight Board Command Language .....	160
RIBCL Sample Scripts.....	160
RIBCL General Guidelines .....	160
XML Header .....	161
Data Types .....	161
String .....	161
Specific String .....	161
Boolean String .....	162
Response Definitions .....	162
RIBCL.....	162
RIBCL Parameter .....	163
RIBCL Runtime Errors.....	163
LOGIN .....	163
LOGIN Parameters .....	164
LOGIN Runtime Errors .....	164
USER_INFO .....	164
USER_INFO Parameter.....	165
USER_INFO Runtime Error.....	165
ADD_USER.....	165
ADD_USER Parameters.....	166
ADD_USER Runtime Errors.....	168
DELETE_USER .....	168
DELETE_USER Parameter.....	169
DELETE_USER Runtime Errors .....	169
GET_USER.....	169
GET_USER Parameter .....	170
GET_USER Runtime Errors.....	170
GET_USER Return Messages .....	170
MOD_USER .....	171
MOD_USER Parameters .....	171
MOD_USER Runtime Errors .....	173

---

GET_ALL_USERS.....	173
GET_ALL_USERS Runtime Error .....	174
GET_ALL_USERS Return Messages .....	174
GET_ALL_USER_INFO.....	175
GET_ALL_USER_INFO Parameters.....	175
GET_ALL_USER_INFO Runtime Errors.....	175
GET_ALL_USER_INFO .....	175
RIB_INFO.....	176
RIB_INFO Parameter .....	176
RIB_INFO Runtime Errors.....	176
RESET_RIB.....	177
RESET_RIB Parameters.....	177
RESET_RIB Runtime Errors.....	177
GET_NETWORK_SETTINGS .....	177
GET_NETWORK_SETTINGS Parameters .....	178
GET_NETWORK_SETTINGS Runtime Errors .....	178
GET_NETWORK_SETTINGS Return Messages.....	178
MOD_NETWORK_SETTINGS.....	179
MOD_NETWORK_SETTINGS Parameters.....	180
MOD_NETWORK_SETTINGS Runtime Errors.....	182
MOD_DIAGPORT_SETTINGS .....	183
MOD_DIAGPORT_SETTINGS Parameters .....	183
MOD_DIAGPORT_SETTINGS Runtime Errors .....	184
DIR_INFO .....	184
DIR_INFO Parameter.....	184
DIR_INFO Runtime Errors .....	184
GET_DIR_CONFIG .....	185
GET_DIR_CONFIG Parameters .....	185
GET_DIR_CONFIG Runtime Errors .....	185
GET_DIR_CONFIG Return Messages.....	185
MOD_DIR_CONFIG.....	186
MOD_DIR_CONFIG Parameters.....	187
MOD_DIR_CONFIG Runtime Errors.....	187
GET_GLOBAL_SETTINGS.....	188
GET_GLOBAL_SETTINGS Parameters.....	188
GET_GLOBAL_SETTINGS Runtime Errors .....	188
GET_GLOBAL_SETTINGS Return Messages .....	188
MOD_GLOBAL_SETTINGS .....	189
MOD_GLOBAL_SETTINGS Parameters .....	189
MOD_GLOBAL_SETTINGS Runtime Errors .....	190
MOD_SNMP_IM_SETTINGS.....	190
MOD_SNMP_IM_SETTINGS Parameters.....	191
MOD_SNMP_IM_SETTINGS Runtime Errors.....	192
CLEAR_EVENTLOG .....	192

CLEAR_EVENTLOG Parameters .....	192
CLEAR_EVENTLOG Runtime Errors .....	193
UPDATE_RIB_FIRMWARE .....	193
UPDATE_RIB_FIRMWARE Parameters .....	193
UPDATE_RIB_FIRMWARE Runtime Errors .....	193
GET_FW_VERSION .....	194
GET_FW_VERSION Parameters .....	194
GET_FW_VERSION Runtime Errors .....	194
GET_FW_VERSION Return Messages .....	195
HOTKEY_CONFIG .....	195
HOTKEY_CONFIG Parameters .....	196
HOTKEY_CONFIG Runtime Errors .....	196
LICENSE .....	197
LICENSE Parameters .....	197
LICENSE Runtime Errors .....	197
RACK_INFO .....	198
RACK_INFO Parameters .....	198
RACK_INFO Runtime Errors .....	198
MOD_BLADE_RACK .....	199
MOD_BLADE_RACK Parameters .....	199
MOD_BLADE_RACK Runtime Errors .....	200
GET_TOPOLOGY .....	200
GET_TOPOLOGY Parameters .....	201
GET_TOPOLOGY Return Message .....	201
SERVER_INFO .....	201
SERVER_INFO Parameter .....	202
SERVER_INFO Runtime Error .....	202
GET_HOST_POWER_STATUS .....	202
GET_HOST_POWER_STATUS Parameters .....	202
GET_HOST_POWER_STATUS Runtime Errors .....	203
GET_HOST_POWER_STATUS Return Messages .....	203
SET_HOST_POWER .....	203
SET_HOST_POWER Parameters .....	203
SET_HOST_POWER Runtime Errors .....	204
RESET_SERVER .....	204
RESET_SERVER Parameters .....	204
RESET_SERVER Errors .....	204
GET_UID_STATUS .....	205
GET_UID_STATUS Parameters .....	205
GET_UID_STATUS Response .....	205
UID_CONTROL .....	205
UID_CONTROL Parameters .....	206
UID_CONTROL Errors .....	206



---

<b>Integrated Lights-Out Parameters</b>	<b>207</b>
Integrated Lights-Out Parameters Table .....	207
Server Identification Parameters .....	211
PCI Resources.....	211
Server Name .....	211
Serial Number.....	212
Firmware Version .....	212
Firmware Date .....	212
User Administration Parameters .....	212
User Name .....	212
Login Name .....	212
Password.....	213
Administer User Accounts.....	213
Remote Console Access .....	213
Virtual Power and Reset .....	213
Virtual Media.....	213
Configure iLO Settings.....	213
Global Settings Parameters .....	214
Idle Connection Timeout (Minutes) .....	214
Enable Lights-Out Functionality .....	214
Enable iLO ROM-Based Setup Utility .....	214
Require Login for iLO RBSU.....	214
Remote Console Port Configuration.....	215
Remote Console Data Encryption.....	215
SSL Encryption Strength .....	215
Current Cipher .....	215
Web Server Non-SSL Port.....	215
Web Server SSL Port.....	215
Virtual Media Port .....	216
Remote Console Port .....	216
Minimum Password Length.....	216
Network Settings Parameters .....	216
Enable NIC .....	216
Transceiver Speed Autoselect.....	216
Speed .....	217
Duplex .....	217
DNS/DHCP .....	217
Registering with WINS Server .....	217
Registering with DNS Server .....	218
Ping Gateway on Startup .....	218
iLO IP Address .....	218
iLO Subnet Mask.....	218

iLO Gateway IP Address .....	218
iLO Subsystem Name .....	218
Domain Name .....	219
DHCP Server .....	219
Primary, Secondary, and Tertiary DNS Server .....	219
Primary and Secondary WINS Server .....	219
Static Route #1, #2, #3 .....	219
Directory Settings Parameters .....	219
Directory Authentication .....	219
Directory Server Address .....	220
Directory Server LDAP Port .....	220
LOM Object Distinguished Name .....	220
LOM Object Password .....	220
Directory User Context 1, Directory User Context 2, Directory User Context 3 .....	220
Testing Directory Settings .....	221
SNMP/Insight Manager Settings Parameters .....	221
SNMP Alert Destinations .....	221
Enable iLO SNMP Alerts .....	222
Forward Insight Manager Agent SNMP Alerts .....	222
Insight Manager Web Agent URL .....	222
Level of Data Returned .....	222
ProLiant BL p-Class Parameters .....	223
Rack Name .....	223
Enclosure Name .....	223
Bay Name .....	223
Bay .....	223
Rack Serial Number .....	224
Enclosure Serial Number .....	224
Blade Serial Number .....	224
Power Source .....	224
Enable Automatic Power On .....	225
iLO Advanced License Activation Settings .....	225
iLO Advanced Pack License Key .....	225

---

## **Troubleshooting Integrated Lights-Out** **227**

Minimum Requirements .....	227
Troubleshooting Alert and Trap Problems .....	228
Inability to Receive Insight Manager 7 Alarms (SNMP Traps) from iLO .....	228
iLO Security Override Switch .....	228
iLO POST LED Indicators .....	229
Hardware and Software Link-Related Issues .....	231
Hardware .....	231
Software .....	232
Login Issues .....	232

Resetting Integrated Lights-Out.....	234
Troubleshooting Video and Monitor Problems .....	234
Troubleshooting Miscellaneous Problems.....	236
Event Log Entries .....	244
<b>Technical Support</b>	<b>249</b>
HP Contact Information .....	249
Before You Contact HP .....	249
<b>Acronyms and Abbreviations</b>	<b>251</b>
<b>Index</b>	<b>255</b>

---

---

# Configuring Integrated Lights-Out

## In This Section

iLO Configuration Options.....	13
Optimizing Performance for Graphical Remote Console.....	16
Enabling iLO Advanced Functionality.....	18
Installing iLO Device Drivers .....	19

## iLO Configuration Options

iLO comes preconfigured with default factory settings, including a default user account and password. If iLO is connected to a network running DNS/DHCP, it can be used immediately without changing any settings.

The majority of the iLO functionality is available in an operating system-independent manner. Some advanced features require that operating system drivers be installed. For greater security, iLO also can be configured using the information in the following sections.

**NOTE:** ProLiant BL p-Class servers may also be accessed through the iLO Diagnostic Port on the front of the server.

iLO offers three configuration options:

- RBSU by pressing the **F8** key

RBSU is the recommended method to initially set up iLO. RBSU is available every time the server is booted and can be run remotely using the iLO Remote Console. You can use RBSU to configure network parameters, directory settings, global settings, and user accounts. RBSU is the required method to initially configure iLO network parameters for environments that do not use DHCP and DNS/WINS.

RBSU can be disabled in the Global Settings preferences. This feature prevents reconfiguration from the host unless the iLO Security Override Switch is set.

- Browser-based setup

You can use this method to initially configure an iLO system that uses DNS/DHCP to obtain an IP address. You can also use this method to reconfigure an iLO that was previously configured.

You can also use this method to initially configure a ProLiant BL p-Class iLO system through the iLO Diagnostic Port.

- Scripted setup

You can use this method to initially configure an iLO system that uses DNS/DHCP to obtain an IP address. Using this method, the configuration of the iLO is sent across the network in a script file using the CPQLOCFG.EXE utility.

## iLO RBSU

**NOTE:** When configuring iLO for the first time, you must use RBSU to setup a non-English keyboard. International keyboards can only be configured using RBSU.

HP recommends using iLO RBSU to initially configure and set up iLO. iLO RBSU is designed to assist you with setting up iLO on a network; it is not intended for continued administration.

To run iLO RBSU:

1. Restart or power up the server.
2. Press the **F8** key when prompted during POST. The iLO RBSU runs.
3. If iLO is configured other than the default, enter a valid iLO user ID and password with the appropriate iLO privileges (**Administer User Accounts, Configure iLO Settings**). Default account information is located on the iLO Default Network Settings tag. If iLO has not been configured to present a login challenge to the RBSU, this step is not necessary.
4. Make and save any necessary changes to the iLO configuration.
5. Exit iLO RBSU.

HP recommends using DNS/DHCP with iLO to simplify installation. If DNS/DHCP cannot be used, use the following procedure to disable DNS/DHCP and to configure the IP address and the subnet mask:

1. Restart or power up the server.

2. Press the **F8** key when prompted during POST. The iLO RBSU runs.
3. Enter a valid iLO user ID and password with the appropriate iLO privileges (**Administer User Accounts, Configure iLO Settings**). Default account information is located on the iLO Default Network Settings tag.
4. Select **Network, DNS/DHCP**, press the **Enter** key, and then select **DHCP Enable**. Press the spacebar to turn off DHCP. Be sure that **DHCP Enable** is set to **Off** and save the changes.
5. Select **Network, NIC and TCP/IP**, press the **Enter** key, and enter the appropriate information in the **IP Address, Subnet Mask** and **Gateway IP Address** fields.
6. Save the changes. The iLO system automatically resets to use the new setup when you exit iLO RBSU.

## Browser-Based Setup

Use this method if you are on a network that uses DHCP/DNS to obtain an IP address. You can also use this method to reconfigure a previously configured iLO.

1. Access iLO from a remote network client using a standard Web browser and provide the default DNS name, user name, and password on the Network Settings tag supplied with the server. The Network Settings tag is usually connected to the outside of the server at shipment.

When you successfully log on to iLO, you can change the default values of the network, user, and SNMP alerting settings through the Web browser interface.

2. Enter the activation key in the browser-based setup to enable iLO Advanced Pack features.

If the iLO Advanced Pack features are licensed, you can deploy your operating system using the Virtual Floppy Drive and install operating system drivers and Insight Manager agents on the remote host server using the graphical Remote Console.

**NOTE:** For ProLiant BL p-Class servers, Integrated Lights-Out Advanced Pack functionality is already enabled and cannot be disabled.

## Optimizing Performance for Graphical Remote Console

The following is a list of recommended client and server settings based on the operating system used.

### Recommended Client Settings

Ideally, the remote server operating system display resolution should be the same resolution, or smaller, than that of the browser computer. Higher server resolutions transmit more information, slowing the overall performance.

Use the following client and browser settings to optimize performance:

- **Display Properties**
  - Select an option greater than 256 colors.
  - Select a greater screen resolution than the screen resolution of the remote server.
  - Linux X Display Properties—On the **X Preferences** screen, set the font sizes to 12.
- **Remote Console**
  - For Remote Console speed, HP recommends using a 700-MHz or faster client with 128 MB or more of memory.
  - For the Remote Console Java applet execution, HP recommends using a single processor client.
- **Mouse Properties**
  - Set the **Mouse Pointer** speed to the middle setting.
  - Set **Mouse Pointer Acceleration** to **low** or disable the pointer acceleration.

## Recommended Server Settings

The following is a list of recommended server settings based on the operating system used.

**NOTE:** To display the entire host server screen on the client Remote Console applet, set the server display resolution less than or equal to that of the client.

### Microsoft® Windows NT® 4.0 and Windows® 2000 Settings

Use the following settings to optimize performance:

- Server **Display Properties**
  - Plain Background (no wallpaper pattern)
  - Display resolution of 800 x 600 or 1024 x 768 pixels
  - 256-color or 24 bit color mode
- Server **Mouse Properties**
  - Select **None** for mouse pointer **Scheme**.
  - Deselect **Enable Pointer Shadow**.
  - Select **Motion** or **Pointer Options** and set the pointer **Speed** slider to the middle position.
  - Set pointer **Acceleration** to **None**.

### Microsoft® Windows Server 2003 Settings

Use the following settings to optimize performance:

- Server **Display Properties**
  - Plain Background (no wallpaper pattern)
  - Display resolution of 800 x 600 or 1024 x 768 pixels
  - 256-color or 24-bit color mode
- Server **Mouse Properties**
  - Select **None** for mouse pointer **Scheme**.



- Select **Disable Pointer Trails**.
- Deselect **Enable Pointer Shadow**.
- Select **Motion** or **Pointer Options**, and set the pointer **Speed** slider to the middle position.
- Deselect **Enhanced Pointer Precision**.

## Red Hat Linux and SuSE Linux Server Settings

Use the following settings to optimize performance:

- Server **Display Properties**
  - 1024 x 768 pixels or lower screen resolution
  - 256 colors
- Server **Mouse Properties**
  - Set **Pointer Acceleration** to **1x**. For KDE, access the **Control Center**, select **Peripherals/Mouse**, then select the **Advanced** tab.
- X Display Properties
  - On the **X Preferences** screen, set the font sizes to 12.

## Novell NetWare Settings

Use the following settings to optimize performance:

### Server **Display Properties**

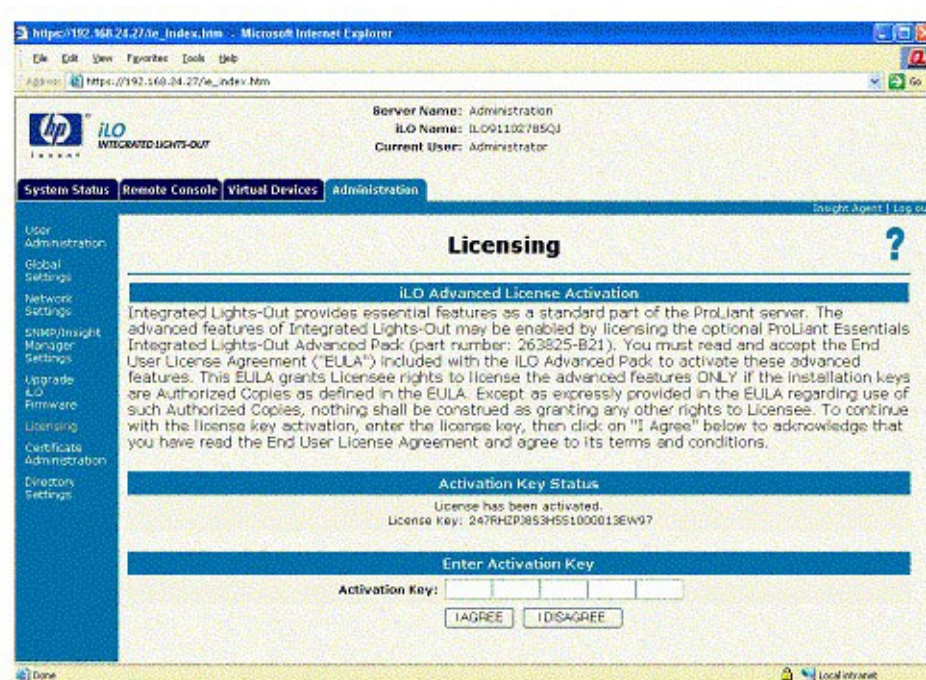
- 800 x 600 pixels or lower screen resolution
- 256 colors

## Enabling iLO Advanced Functionality

The iLO Advanced functionality is enabled by licensing the optional iLO Advanced Pack. The iLO Advanced Pack contains an activation key that you must enter into iLO to enable advanced functionality.

To enable the iLO advanced functionality:

1. Log on to iLO through a supported Web browser.
2. Click the **Administration** tab.
3. Click **Licensing** to display the iLO Advanced License Activation screen.



4. Enter the activation key into the space provided.
5. Click **I Agree**.

The advanced features of iLO are now enabled.

## Installing iLO Device Drivers

A majority of the iLO functionality is available without any operating system-based software or drivers. Two driver interfaces, however, are provided to the iLO management processor.

- The first interface is for the iLO Advanced System Management Driver. This driver is also known as the Health Driver and provides system management support, including monitoring of server components, event logging, and support for the HP Management Agents.
- The second interface is for the iLO Management Interface Driver. This driver allows system software and SNMP Insight Agents to communicate with the iLO.

The following sections provide instructions for installing iLO drivers for:

- Microsoft®
- Novell
- Linux

Refer to the HP website (<http://www.hp.com/support>) for the latest versions of these drivers.

## **Microsoft Windows NT, Windows 2000, and Windows Server 2003 Driver Support**

The device drivers that support the iLO are part of the PSP that is located on the HP website (<http://www.hp.com/support>) or on the SmartStart CD. Before you install the Windows® drivers, obtain the Windows® documentation and the latest Windows® Service Pack.

### **Microsoft® Relevant Files**

The CPQCIDRV.SYS file provides the iLO Management Interface Driver support.

The CPQASM2.SYS, SYSMGMT.SYS, SYSDOWN.SYS files provide the iLO Advanced Server Management Controller Driver support.

### **Installing or Updating the iLO Microsoft® Drivers**

The PSP for Microsoft® Windows® products includes an installer that analyzes system requirements and installs all drivers.

The PSP is available on the HP website (<http://www.hp.com/support>) or on the SmartStart CD.

**NOTE:** If you are updating the iLO drivers, be sure that the iLO is running the latest version of the iLO firmware. The latest version can be obtained as a Smart Component from the HP website (<http://www.hp.com/servers/lights-out>).

To install the drivers in the PSP, download the PSP from the HP website (<http://www.hp.com/support>), run the SETUP.EXE file included in the download, and follow the installation instructions. For additional information about the PSP installation, read the text file included in the PSP download.

## Novell NetWare Server Driver Support

The device drivers required to support iLO are part of the PSP that is located on the SmartStart CD and the HP website (<http://www.hp.com/support>).

### NetWare Relevant File

The CPQHLTH.NLM file provides the Health Driver for NetWare.

The CPQCI.NLM file provides the iLO Management Interface Driver support.

### Installing or Updating iLO NetWare Drivers

The PSP for Novell NetWare includes an installer that analyzes system requirements and installs all drivers. The PSP is available on the HP website (<http://www.hp.com/support>) and on the SmartStart CD.

**NOTE:** If you are updating the iLO drivers, be sure that the iLO is running the latest version of the iLO firmware. The latest version can be obtained as a Smart Component from the HP website (<http://www.hp.com/servers/lights-out>).

To install the drivers, download the PSP from the HP website (<http://www.hp.com/support>) to a NetWare server. After the PSP has been downloaded, follow the NetWare component installation instructions to complete the installation. For additional information about the PSP installation, read the text file included in the PSP download.

**NOTE:** When using NetWare 6.X, a RAGE-IIC video driver is provided by the operating system and should be used for best results.

## Red Hat Linux and SuSE Linux Server Driver Support

The device drivers required to support iLO for Red Hat Linux and SuSE Linux are located on the SmartStart CD, Management CD, or on the HP website (<http://www.hp.com/support>).

### Relevant Files

You can download the PSP files containing the iLO driver, the foundation agents, and health agents from the HP website (<http://www.hp.com/support>). The instructions on how to install or update the iLO driver are available on the website. The HP Management Agents for Linux are:

- ASM package 6.20.0 or later (hpasm) which combines the health driver, IML viewer, foundation agents, health agent, and standard equipment agent into one package.
- RSM package 6.20.0 or later (hprsm) which combines the RIB driver, rack daemon, RIB agent, and rack agent into one package.

These packages cannot upgrade previous versions of the agents and drivers. Remove previous agents before applying the new agents. Uninstall the agents and drivers by using the following commands:

- `rpm -e cpqrcki`
- `rpm -e cmanic`
- `rpm -e cmastor`
- `rpm -e masvr`
- `rpm -e cmafdtn`
- `rpm -e cpqhealth`

Download and install the HP Linux Management Agents. An example of the package name is hpasm-6.20.0-11.Redhat7\_3.i386.rpm

Use the following commands to load the packages:

```
rpm -ivh hpasm-d.vv.v-pp.Linux_version.i386.rpm  
rpm -ivh hprsm-d.vv.v-pp.Linux_version.i386.rpm
```

where: *d* is the Linux distribution and version and

*vv.v-pp* are version numbers.

For additional information, refer to the Software and Drivers website (<http://www.hp.com/support>).

If necessary, you can uninstall, stop, or start the iLO by using the following commands:

- Uninstall  

```
rpm -e cpqci
```
- Stop  

```
/etc/rc.d/init.d/cpqci stop
```
- Start  

```
/etc/rc.d/init.d/cpqrci start
```

For additional information, refer to the Software and Drivers website (<http://www.hp.com/support>).

# Using Integrated Lights-Out

## In This Section

Supported Server Operating System Software .....	25
Supported Browsers.....	26
Single and Dual Cursor Modes for Graphical Remote Console.....	27
Common Usage Model.....	28
Connection Overview .....	29
Operational Overview.....	30
Accessing iLO for the First Time .....	35
System Status.....	40
Remote Console.....	45
Virtual Devices .....	50
Administration .....	63
ProLiant BL p-Class .....	77
Telnet Support .....	83

## Supported Server Operating System Software

iLO is an independent microprocessor running an embedded operating system. This architecture ensures that the majority of the iLO functionality is available regardless of the host operating system.

Graceful host operating system shutdown and Insight Manager 7 integration require Health Drivers and Management Agents.

iLO provides interfaces for two drivers:

- Advanced Server Management Controller Driver
- iLO Management Interface Driver

These drivers and agents are available for the following network operating systems:

- Microsoft®

- Windows NT® 4.0 Server
  - Windows NT® 4.0, Enterprise Edition
  - Windows® 2000 Server
  - Windows® 2000 Advanced Server
  - Windows® Server 2003
- Linux
  - Red Hat 7.3
  - Red Hat 8.0
  - Red Hat 9
  - Red Hat Server 2.1
  - SuSE SLES 7.0
  - SuSE SLES 8.0
- Novell
  - NetWare 5.x
  - NetWare 6

## Supported Browsers

- Microsoft® Internet Explorer
  - Minimum: Microsoft® Internet Explorer 5.5 with with Service Pack 2 or later for Windows® 2000 or Windows® XP. If using single cursor mode in Remote Console, Java™ 1.3.1\_02 or greater JVM is required.
  - Recommended: Microsoft® Internet Explorer 6.0 or later and Java™ 1.4.X JVM for Windows® 2000 or Windows® XP. To download the recommended JVM for your system configuration, refer to the HP website (<http://www.hp.com/servers/manage/jvm>).
- Linux
  - Netscape 7.x



- Mozilla 1.2.1

Linux, Netscape and Mozilla require Java™ 1.4.1 JVM or later. To download the recommended JVM for your system configuration, refer to the HP website (<http://www.hp.com/servers/manage/jvm>).

Certain browsers and operating system combinations might not work correctly depending on their implementations of the required browser technologies.

## Single and Dual Cursor Modes for Graphical Remote Console

The Graphical Remote Console can utilize either a single or dual cursor mode.

### Remote Console (Dual Cursor)

The Remote Console dual cursor option uses two mouse cursors in the Remote Console window to represent the mouse cursor of the remote server and the mouse cursor of the local client. The local client cursor is seen as a crosshair in the Remote Console window. The dual cursor option is supported with Java™ 1.1 VM and later. If the two cursors drift apart, they can be synchronized and brought back together. To synchronize the remote and local cursors:

1. Right-click, drag, and move the local crosshair cursor to align with the mouse cursor of the remote server.
2. Holding the **Ctrl** key, move the local crosshair cursor to align with the mouse cursor of the remote server.

You might prefer the dual cursor option because you can see where the cursor exits the Remote Console applet window. HP recommends using the Remote Console dual cursor mode with text-based operating systems.

### Remote Console (Single Cursor)

The Remote Console option presents a single mouse cursor during a Remote Console session. Synchronization of two cursors is eliminated, making navigation easier in the Remote Console window.

Single Cursor mode requires Java™ 1.3.1\_02 JVM or later for Microsoft® Internet Explorer, and Java™ 1.4.1 JVM for Netscape and Mozilla. To download the recommended JVM for your system configuration, refer to the HP website (<http://www.hp.com/servers/manage/jvm>).

**NOTE:** You will be redirected from the main site to the java.sun.com site. HP recommends using the version specified in the Remote Console help pages. You can obtain the specified version for Internet Explorer either from the java.sun site or on the Management CD.

## Common Usage Model

The common usage model for iLO is a client PC running a supported browser connected over an external network to one or more iLO devices. Through DHCP and DNS, iLO is ready to use by plugging in the power of the host server and connecting an Ethernet cable to the dedicated iLO management port of the server. You can then use your Web browser to connect to iLO over an SSL connection. When logged in, you can remotely control the server from your client desktop.

Using a supported Web browser, you can:

- Remotely access the console of the host server in text mode only.
- Remotely access the console of the host server in graphical mode with full keyboard and mouse controls (if licensed with the iLO Advanced Pack).
- Remotely power up, power down, or reboot the host server.
- Remotely boot a host server to a virtual CD or virtual floppy image to perform a ROM upgrade or to install an operating system (if licensed with the iLO Advanced Pack).
- Send alerts from iLO regardless of the state of the host server.
- Access troubleshooting features provided by iLO.
- Launch a Web browser, use SNMP alerting, and diagnose iLO using Insight Manager 7.

This section describes how to access the iLO features with a supported Web browser. All features are fully discussed and descriptions of all iLO configuration settings are given.

Graphical Remote Console and Virtual Media are advanced functions that must be enabled by licensing the optional iLO Advanced Pack. Advanced features are described and annotated.

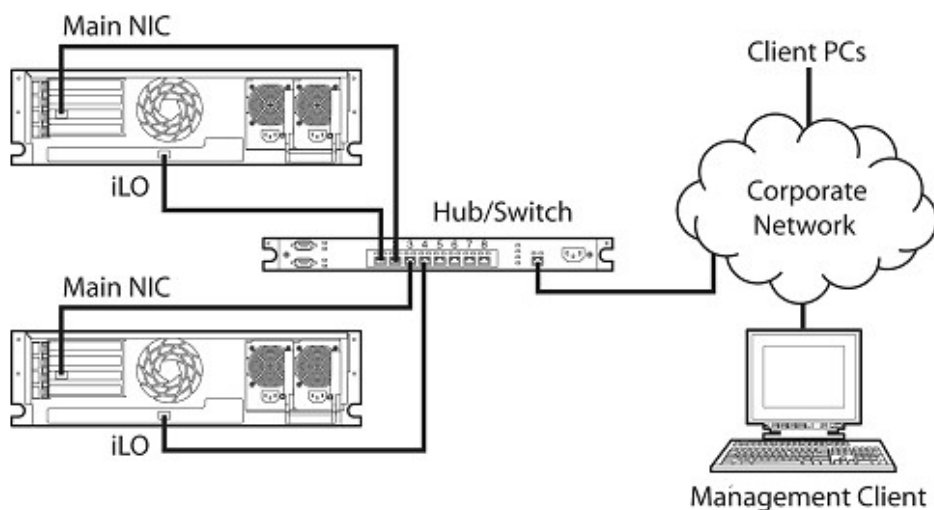
## Connection Overview

The servers in the following examples are equipped with two ports: a 10/100/1000-Mbps NIC and a 10/100-Mbps iLO port. The two general scenarios are to either connect both ports on a corporate network or to connect the iLO port to a separate iLO network. The following is a discussion of the benefits and drawbacks of using each scenario.

### Corporate Network Connection

The server has two ports that can be connected to a corporate network. This connection allows access to iLO from anywhere on the network. On a corporate network, however, network traffic can hinder iLO performance.

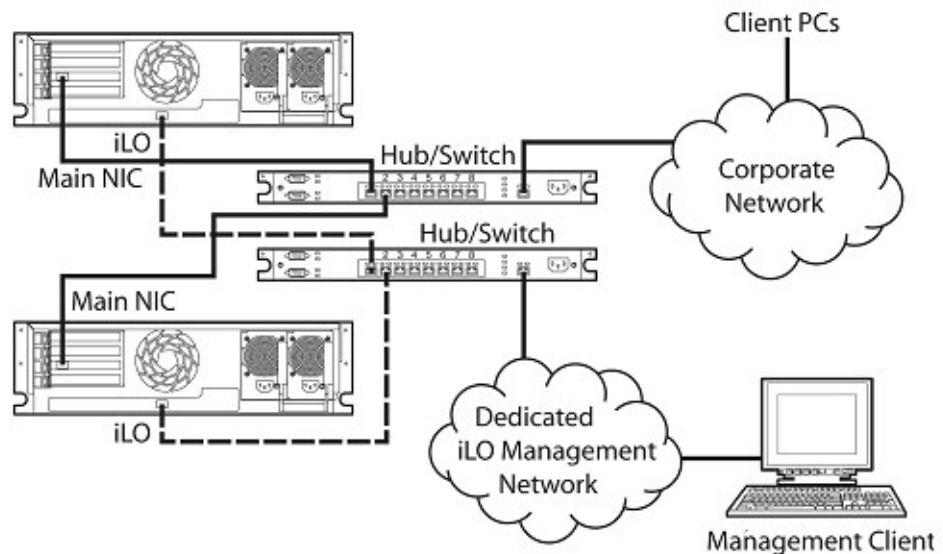
This configuration reduces the amount of networking hardware and infrastructure required to support iLO. Configured in this manner, iLO can use existing DNS/DHCP servers and routers.



## Integrated Lights-Out Network Connection

Integrated Lights-Out can be on a separate dedicated management network. A separate network allows for a performance benefit, but iLO cannot be accessed directly from the corporate network under this configuration.

A dedicated management network can also be used to increase the security of the iLO port. A separate network enables you to physically control which workstations are connected to management network.



## Operational Overview

- Virtual text Remote Console

The standard iLO provides embedded hardware Remote Console capabilities on a text mode screen. The operating system-independent console supports text modes that display remote host server activities, such as shutdown and startup operations.

- Virtual graphical Remote Console (if licensed with the iLO Advanced Pack)

iLO provides embedded hardware graphical Remote Console capabilities that turn a supported browser into a virtual desktop, giving the user full control over the display, keyboard, and mouse of the host server. The operating system-independent console supports graphic modes that display remote host server activities, such as shutdown and startup operations.

- **Power Cycle (Reset)**

If the remote host server is not responding, this feature enables an administrator to initiate a cold or warm reboot to bring the server back online.

- **Virtual Media (if licensed with the iLO Advanced Pack)**

With the Virtual Floppy Drive or Virtual CD Drive, an administrator can direct a remote host server to boot and use standard media from anywhere on the network, thus saving time and increasing efficiency by eliminating the need to visit a remote server to insert and use a diskette. Administrators can carry out any of the following functions remotely:

- Applying ROMPaq upgrades to remote servers
- Deploying an operating system on remote servers from the Virtual CD Drive, network drives, or by using the SmartStart Scripting Toolkit

- **Virtual Power Button**

With a supported browser interface, iLO can be used to remotely operate the power button of a host server.

- **Virtual Serial Port**—Provides a Java™ applet that allows connection to the server serial port. The Java™ applet provides VT320 terminal emulation to access an application configured for the serial port. The Virtual Serial Port can be used for Windows® Server 2003 EMS.
- **Directory Services support (if licensed with iLO Advanced Pack)**—Enables login to iLO using Active Directory or eDirectory accounts. Snap-ins to MMC and ConsoleOne centralize and simplify the management of authentication and authorization to Lights-Out Management devices.
- **Remote Firmware Update**

This feature enables you to keep iLO current with the latest firmware available from HP. Updates to the ROM code on iLO are accomplished through the browser interface.

- Integration with Insight Manager 7

Insight Manager 7 provides full integration with iLO. This integration includes:

- Support for SNMP trap delivery to an Insight Manager 7 console
- Support for SNMP management

Insight Manager 7 is allowed to access the Insight Management Agents information through iLO.

- Support for a management processor

Insight Manager 7 adds support for a new device type, the management processor. All iLO devices installed in servers on the network are discovered in Insight Manager 7 as management processors. The management processors are associated with the servers in which they are installed.

- Grouping of iLO management processors

All iLO devices can be grouped together logically and displayed on one page. This capability provides access to iLO from one point in Insight Manager 7.

- iLO hyperlinks

Insight Manager 7 provides a hyperlink on the server device page to launch and connect to iLO.

- HP Management Agents

iLO, combined with HP Management Agents, provides remote access to system management information through the iLO Web browser interface.

- ProLiant BL p-Class Support

- iLO provides ProLiant BL p-Class rack information to allow Insight Manager 7 to draw a graphical representation of the rack.

- Integration with RILOE II option boards

The RILOE II board is supported as an option in servers with iLO. Previous generations of the Remote Insight boards, such as the Remote Insight board/PCI and the original RILOE board, are not supported in servers with iLO.

Integrated Lights-Out firmware version 1.10 or higher will detect the presence of the RILOE II and automatically disable the iLO functionality. Additionally, iLO firmware version 1.10 and higher will detect the presence of the original RILOE and display an invalid configuration message.

To re-enable the iLO functionality after a RILOE II is removed, the Security Override Switch and the F8 ROM-Based Setup Utility for iLO must be used. Select **Settings** and then select **Enabled** for the "Lights-Out Functionality" setting.

- Dedicated LAN network connectivity

A 10/100-Mbps Ethernet chip on iLO provides administrators with a dedicated network connection. iLO provides in-band SNMP notification of server problems on a real-time basis without separate telephone connections or modem sharing devices. The NIC can auto-select speeds between 10 Mbps and 100 Mbps.

- Scripted configuration of iLO

All settings of iLO, including user settings, network settings, global settings, and SNMP/Insight Manager settings, can be configured through script files. Scripting can be launched from a Windows® client or, integrated with the SmartStart Scripting Toolkit, the ProLiant Essentials Rapid Deployment Pack, or Insight Manager 7.

- Dial-up support

iLO is available through dial-up access when using a modem router or external RAS connection to log on to the network.

- VPN support

iLO functionality is available around the world when used in conjunction with VPN technology.

- SNMP alerts from iLO to a management console

Using a management console, you can access certain server alerts, such as SNMP alerts and unauthorized access alerts.

- User administration and security

iLO supports up to 12 users with customizable access rights, login names and advanced password encryption. Individual user's abilities are controlled by privileges. Each user may have privileges custom-tailored to their access requirements.

To support more than 12 users, iLO Advanced 1.40 and later allows integration with directory-based user accounts. This enables virtually unlimited user accounts.

iLO provides secure password encryption, tracking all login attempts and maintaining a record of all login failures. When login attempts fail, iLO also generates alerts and sends them to a remote management console. iLO also provides the following security features:

- User defined TCP/IP ports
- User actions logged in the iLO Event Log
- Progressive delays for failed login attempts
- 128-bit encryption of Web pages and Remote Console data

iLO provides strong security for remote management in distributed IT environments by using industry-standard SSL encryption of HTTP data transmitted across the network. SSL encryption (up to 128-bit) ensures that the HTTP information is secure as it travels across the network.

SSL is a network protocol layer, located directly under the application layer, with responsibility for the management of a secure (encrypted) communication channel between the client and server.

Remote Console data is protected using 128-bit RC4 bi-directional encryption.

- Auto configuration of IP address using DNS/DHCP

iLO provides automatic network configuration. iLO comes with a default name and DHCP client that leases an IP address from the DHCP server on the network. For systems that do not use DNS/DHCP, iLO allows static IP configuration.

The default user name, password, and DNS name are:

User name: Administrator

Password: A random, eight-character, alphanumeric string



DNS name: *ILOXXXXXXXXXXXX* where the 12 Xs represent the serial number of the server in which the iLO processor is located. The DNS name of iLO is configurable by the user.

**NOTE:** User names and passwords are case sensitive.

- **IML**

iLO manages the IML of the server, which can be accessed by using a supported browser, even when the server is not operational. This capability can be helpful when troubleshooting remote host server problems.

- **RBSU F8**

This versatile, system-independent RBSU enables fast and easy setup of iLO.

- **Single mouse cursor mode**

Single Cursor mode requires Java™ 1.3.1\_02 JVM or later for Microsoft® Internet Explorer, and Java™ 1.4.1 JVM for Netscape and Mozilla. To download the recommended JVM for your system configuration, refer to the HP website (<http://www.hp.com/servers/manage/jvm>).

**NOTE:** You will be redirected from the main site to the java.sun.com site. HP recommends using the version specified in the Remote Console help pages. You can obtain the specified version for Internet Explorer either from the java.sun site or on the Management CD.

- **HP ProLiant BL p-Class**

This setting enables you to manage the Rack, Enclosure, and Bay names for easier identification, as well as control power source options and rack alert options. Diagnostic information for the server blade management module and the power management module are also available. This tab is displayed only if you are using a supported ProLiant BL p-Class server.

## Accessing iLO for the First Time

iLO is configured with a default user name, password, and DNS name. A network settings tag with the preconfigured values is attached to the server containing the iLO management processor. Use these values to access iLO remotely from a network client using a standard Web browser.

**IMPORTANT:** For security reasons, HP recommends changing the default settings after accessing iLO for the first time.

The default values are:

- User name: Administrator
- Password: A random, eight-character, alphanumeric string
- DNS name: *ILOXXXXXXXXXXXX*, where the 12 Xs represent the serial number of the server

**NOTE:** User names and passwords are case sensitive.

To access iLO for the first time:

1. Enter the iLO IP address or DNS name in the address bar of the Web browser.

**NOTE:** This procedure assumes that your network supports DNS/DHCP. If not, you must configure the IP address using the RBSU or, for ProLiant BL p-Class servers, through the iLO Diagnostic Port.

2. When connecting to iLO in a browser for the first time, you will receive a security alert, as shown.



3. This alert is displayed because the default SSL certificate that is dynamically generated by iLO is not known to the browser. You can view and install the certificate or click **Yes** every time you want to access iLO.

**NOTE:** Refer to the "Certificates (on page 97)" section to import a certificate signed by a CA.

4. If you click **Yes**, the browser continues to the login screen of iLO. The alert message displays each time that you access the iLO management processor in a browser.
5. If you click **No**, you are returned to the **Welcome** screen of iLO.
6. If you click **View Certificate**, a popup window displays the certificate information, as shown. Installing the default certificate onto the browser prevents the security alert message from being displayed in the future.
7. To install the certificate, proceed to step 8. If you choose not to install the certificate, proceed to step 9.



**NOTE:** If the certificate is removed from your browser, if you have upgraded the firmware, or if iLO is rebooted, the security alert message will be displayed again.

8. Install the default certificate to your browser:

- a. Click **Install Certificate**. The Certificate Import Wizard starts.
  - b. Click **Next**.
  - c. Click **Next** for the browser to automatically select the certificate store when the **Certificate Store** window is displayed.
  - d. Click **Finish** when the **Completing the Certificate Import Wizard** window is displayed.
  - e. Click **Yes** to confirm the installation of the default certificate when the confirmation window is displayed.
  - f. Click **OK** to acknowledge that the certificate import was successful.
  - g. Click **OK** in the **Certificate** window to return to the **Security Alert** window.
  - h. Click **Yes** in the **Security Alert** window to log in.
9. When the browser completes the SSL connection to iLO, the **Account Login** screen prompts you for a user name and password. Use the default user name and password from the Network Settings tag and click **Log In**.



**Account Login**

This is a private system. Do not attempt to login unless you are an authorized user.  
Any authorized or unauthorized access and use may be monitored and can result in criminal or civil prosecution under applicable law.

Login Name:

Password:

Copyright © 2003 Hewlett-Packard Development Company, L.P.

Hewlett-Packard and the Hewlett-Packard logo are trademarks of Hewlett-Packard Development Company, L.P. in the U.S. and/or other countries.

Confidential computer software. Valid license from Hewlett-Packard required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Contains security software licensed from: RSA Data Security Inc.  
Portions Copyright 1985, 1991, 1992 by Carnegie Mellon University  
Derivative Work - 1996, 1998-2000 Copyright 1996, 1998-2000 The Regents of the University of California

10. After the default user name and password have been verified, the **Status Summary** screen is displayed.



**NOTE:** The **BL p-Class** is not illustrated in this and subsequent screen shots.

The iLO **Status Summary** provides general information about iLO, such as the user currently logged on, server name and status, iLO IP address and name, and latest log entry data. The **Status Summary** screen also shows whether iLO has been configured to use HP Web-Based Management and Insight Management Web agents.

## Progressive Delays for Failed Browser Login Attempts

After an initial failed login attempt, iLO imposes a delay of five seconds. After a second failed attempt, iLO imposes a delay of 10 seconds. After the third failed attempt, iLO imposes a delay of 60 seconds. All subsequent failed login attempts cycle through these values. An information page is displayed during each delay. This scenario continues until a valid login is completed.

This feature assists in defending against possible dictionary attacks against the browser login port.

## Help

Assistance for all iLO options is available by means of the iLO Help option. These links provide summary information about the features of iLO and helpful information for optimizing its operation. To access page-specific help, click the ? on the right side of the browser window.

## System Status

The following options are available within the **System Status** tab and, enable you to see general and detailed server status information, view event and management log data, and view diagnostic data.

## Status Summary

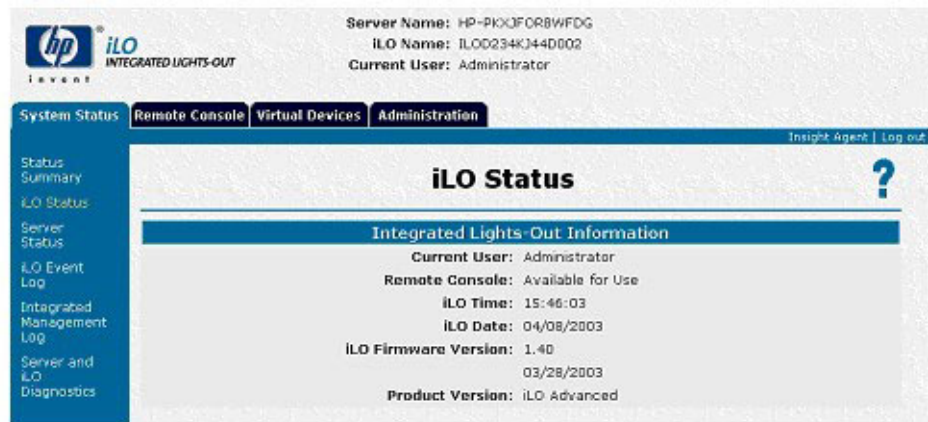
The **Status Summary** screen provides general information about iLO, such as the current user, server name and status, iLO IP address and name, and latest log entry data.

## iLO Status

The **iLO Status** option provides comprehensive iLO status information, including:

- The current user
- The status and availability of the Remote Console
- The date and time currently in use by iLO
- The revision information of the iLO firmware

- The product version (iLO Standard or iLO Advanced) of iLO

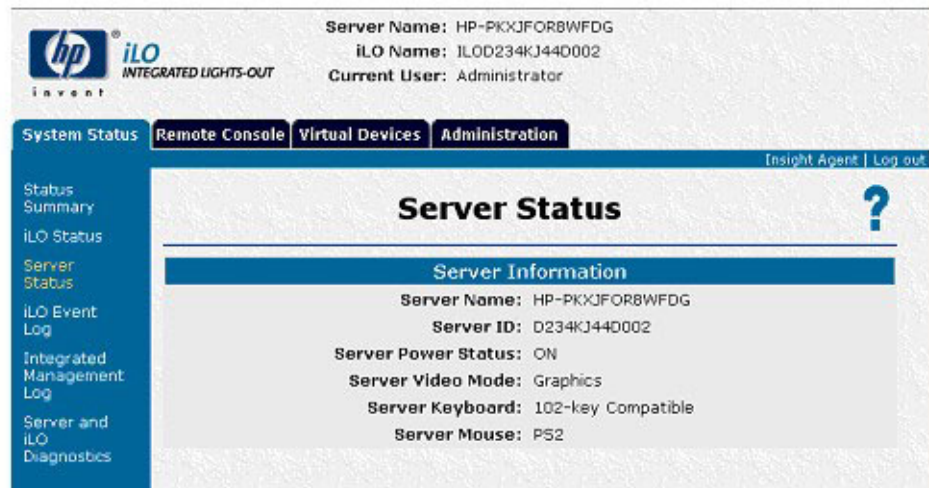


## Server Status

The **Server Status** option provides comprehensive status information about the server, including:

- Server name associated with the iLO management processor  
**NOTE:** The **Server Name** field reports host is `unnamed` if the HP Management Agents are not loaded on the host server.
- Server power status
- Server video mode

- Server keyboard and mouse type



## iLO Event Log

The iLO Event Log is an operating system-independent log that maintains a record of events by date and time. Logged events include major server events, such as a server power outage or a server reset, and iLO events, such as an unauthorized login attempt.

Other events logged include any successful or unsuccessful browser and Remote Console logins, virtual power and power cycle events, and clear event log actions. Some configuration changes, such as creating or deleting a user, are also logged.

Clicking **Clear Event Log** clears the iLO event log of all previously logged information. Click **OK** to confirm that you want to clear the event log. A line indicating that the log has been cleared is logged.

**NOTE:** Events logged by higher versions of iLO firmware may not be supported by lower version firmware. If an event is logged by an unsupported firmware, the event will be listed as UNKNOWN EVENT TYPE. You may clear the event log to eliminate these entries, or update firmware to the latest supported version to resolve this cosmetic issue.



## Integrated Management Log

The IML enables you to view logged remote server events. Logged events include all server-specific events recorded by the system health driver, including operating system information and ROM-based POST codes. For more information, refer to the server guide.

Clicking **Clear Event Log** clears the IML event log of all previously logged information. Click **OK** to confirm that you want to clear the event log. A line indicating that the log has been cleared is logged.

## Server and iLO Diagnostics

The **Server and iLO Diagnostics** option provides comprehensive diagnostic information, as described in the following sections.

**NOTE:** When connected through the Diagnostics Port, the directory server is not available. You can log in using a Local account only.

### POST Diagnostic Results for the Host Server

As an integrated management processor, iLO monitors the progress of the boot process of the server. The host server ROM writes POST codes as it is booting. iLO records and displays these codes. Selected POST codes are considered to be milestone codes and will have a description associated with them. You may use these milestone codes and descriptions to determine how far the server progressed through the boot process.

The POST codes document the booting process of the ROM bios. A code indicates the start of a particular phase of the boot process. The POST code results can be used to determine the general phase in which the boot process stopped. Use of the POST codes alone is usually not sufficient to diagnose the actual root cause of a stopped boot process. The POST codes should be used in conjunction with other tools, such as the IML, the local or iLO Remote Console, and the Diagnostic utilities to determine the root cause of a stopped boot process.

The following list includes all of the POST codes and Diagnostic Results for the host server tracked by iLO for a routine boot sequence on ProLiant servers.

<b>Code</b>	<b>Start of Phase</b>
FE04	EISA Initialization
FE08	PCI Initialization
FE0C	Processor Initialization
FE10	Video Initialization
FE14	Cache Initialization
FE18	USB Initialization
FE1C	Memory Test
FE20	Memory Initialization
FE24	USB Startup
FE28	Floppy Controller Test
FE2C	Option ROM Initialization
FE30	ATAPI Option ROM Initialization
FE34	BBS Initialization
FE38	Begin BOOT Process
FE3C	Attempting SCSI CD Boot
FE40	Attempting Floppy Boot
FE44	Attempting HD Boot
FE48	Attempting CD Boot
FE4C	Attempting PXE Boot
FE50	Passing control to boot sector code
FE54	No bootable devices

## **NVRAM Environment Variables Listing**


HP uses NVRAM to store server environment variable information. This information can be useful to HP engineers and advanced customers who have detailed knowledge of HP System Management architecture.

## Virtual NMI Button

The Virtual NMI button halts the operating system for debugging purposes. This is an advanced feature that should only be used by kernel debuggers.

## iLO Self-Test Results

The results of the iLO Self-Test are displayed in this section of the Web page. All tested subsystems should display Passed under normal situations.



Server Name: HP-PKXJFOR8WFDG  
iLO Name: ILOD234KJ44D002  
Current User: Administrator

System Status Remote Console Virtual Devices Administration

Insight Agent | Log out

### Server and iLO Diagnostics

POST results for server NVRAM environment variables Virtual NMI Button iLO self-test results

#### POST diagnostic results for the host server

Code	Description
FE1C	Memory Test
FE20	Memory Initialization
FE24	USB Startup
FE28	Floppy Controller Test
FE2C	Option ROM Initialization
FE30	ATAPI Option ROM Initialization
FE34	BBS Initialization
FE38	Begin BOOT Process
FE48	Attempting CD Boot
FE54	No bootable devices
FE40	Attempting Floppy Boot

## Remote Console

The following is a list of the options available within the **Remote Console** tab, which provides access to different views of the Remote Console and enables you to define keystroke sequences that will be transmitted to the remote host server at the press of a hot key. Text mode is standard. The Graphical Remote Console can be enabled by licensing the iLO Advanced Pack.

## Remote Console Information Option

The **Remote Console Information** option displays information concerning the Remote Console options available, as well as a link to download an updated Java™ Runtime Environment, which is necessary for using Remote Console with the single cursor option ("Single Mouse Pointer in the Remote Console" on page 48).

The **Remote Console Information** option also displays whether the Remote Console is in use or is available. Although up to 10 users are allowed to simultaneously log in to iLO, only one user at a time can access the Remote Console. A warning message is displayed to say the Remote Console is already in use.

**NOTE:** You can only open either a Telnet session or a Remote Console Session at a time, not both simultaneously. An error message will generate if both sessions are attempted at the same time.

**NOTE:** Remote console will not be available if the remote console port configuration on the **Global Settings** tab is set to disabled.

## Remote Console Option

The **Remote Console** option redirects the host server console to the network client browser, providing full text (standard) and graphical mode video, keyboard, and mouse access to the remote host server (if licensed with the iLO Advanced Pack).

With the Remote Console, you have complete control over a remote host server as if you were in front of it. You can access the remote file system and the network drives. The Remote Console enables you to change hardware and software settings of the remote host server, install applications and drivers, change remote server screen resolution, and gracefully shut down the remote system.

With the Remote Console, you can observe POST boot messages as the remote host server restarts and initiate ROM-based setup routines to configure the hardware of the remote host server. When installing operating systems remotely, the graphical Remote Console (if licensed) enables you to view and control the host server screen throughout the installation process.

For best performance, be sure to configure the host operating system display as described in "Optimizing Performance for Graphical Remote Console (on page 16)."



## Enhanced Features of the Remote Console

The Remote Console applet contains four buttons that provide iLO with enhanced features. These buttons have the following functions:

- **Refresh**—Because there might be instances when the **Remote Console** screen is not displaying the latest data, click **Refresh** to force iLO to repaint the screen.
- **Ctrl-Alt-Del**—Use this button to enter the key sequence **Ctrl+Alt+Del** into the Remote Console.

- **Alt Lock**—Use the **Alt Lock** box to transmit a key sequence beginning with **Alt** to the server from the Remote Console session.
- **Character Set**—Use this menu to change the default character set used by the Remote Console. Modifying the Remote Console character set ensures the correct display of characters.

## Single Mouse Pointer in the Remote Console

One feature of the Remote Console is a single mouse pointer, which means that the local cursor is not displayed when the mouse cursor is over the Remote Console screen.

For this feature to work properly, you must download Java™ 1.3.1 JVM or later for Internet Explorer or 1.4.1 JVM for Linux browsers, and install it on the client machine. The remote server does not require any other software to obtain a single mouse pointer. You can download Java™ 1.3.1 JVM from the HP website (<http://www.hp.com/servers/manage/jvm>).

Linux users should use the 1.4.1 Java2™ Runtime Environment, Standard Edition also available on the HP website (<http://www.hp.com/servers/manage/jvm>).

**NOTE:** You will be redirected from the main site to the java.sun.com site. HP recommends using the version specified in the Remote Console help pages. You can obtain the specified version for Internet Explorer either from the java.sun site or on the Management CD.

Links to download the required JVMs are available on the Remote Console Information screen.

## Remote Console Linux Settings

When using the iLO Remote Console to display text screens in Linux, border characters or other line drawing characters might not display correctly.

To properly configure the Remote Console text mode character set

- Click the **Character Set** pull-down menu from the Remote Console applet.
- Select the **Lat1–16** character set.

## Remote Console (Dual Cursor) Mode

All the features discussed in the "Remote Console (on page 45)" section are available when using Remote Console (dual cursor). When selecting this option, there will be two cursors on the screen: the main cursor and a secondary cursor within the Remote Console (dual cursor) frame. When passing the main cursor across the Remote Console frame, the secondary cursor will track to the main cursor.

The mouse cursor of the client computer is displayed within the Remote Console as a cross-hair symbol. Some iLO users prefer to see exactly where the client computer mouse cursor is located. For best performance, be sure to configure the host operating system display as described in "Optimizing Performance for Graphical Remote Console (on page 16)".

The Remote Console (dual cursor) option is your only Remote Console option if you choose not to download an updated Java™ Runtime Environment.

## Remote Console Hot Keys

The Remote Console hot keys feature enables you to define up to six multiple key combinations to be assigned to each hot key. When a hot key is pressed in the Remote Console, on client systems, the defined key combination (all keys pressed at the same time) will be transmitted in place of the hot key to the remote host server.

To define a Remote Console hot key:

1. Click **Remote Console Hot Keys** in the **Remote Console** tab.
2. Select the hot key you want to define and use the drop-down boxes to select the key sequence to be transmitted to the host server at the press of the hot key.
3. Click **Save Hot Keys** when you have finished defining the key sequences.

The **Remote Console Hot Keys** screen also contains a **Reset Hot Keys** option. This option clears all entries in the hot key fields. Click **Save Hot Keys** to save the cleared fields.

**NOTE:** The Remote Console Hot Keys are active during a remote console session via the Remote Console applet and during a text remote console session via a telnet client.

## Troubleshooting a Remote Host

Troubleshooting a remote host server may require restarting the remote system. You can restart the remote host server by using the options listed in the **Virtual Devices** tab. Both options display the current power status of the server.

## Virtual Devices

The following is a list of the options available within the **Remote Console** tab, which provides remote Virtual Power Button, Virtual Media, and Virtual Indicators capabilities. Virtual Media can be enabled by licensing the iLO Advanced Pack.



## Virtual Power Button

The **Virtual Power** button allows control of the power state of the remote server and simulates pressing the physical power button on the server. To use the **Virtual Power** button, select the power option that you want and click **Virtual Power** button to initiate the power option.



**NOTE:** Some of these features will not gracefully shut down the operating system. An operating system shutdown should be initiated using the Remote Console before using the Virtual Power Button.

Use the refresh feature of the browser to keep the status of the power indicator up to date.

The available power options are:

- **Momentary Press**—This option simulates a momentary press of the power button. A momentary press is usually sufficient to turn off a server that is currently on or to turn on a server that is currently off. To use this option, select **Momentary Press** and click the **Virtual Power** button.

- **Press and Hold**—This option presses and holds the power button for six seconds, which is useful in forcing the system to power off if the operating system is not responding to the momentary press. To reboot the system, select **Cold Boot of system** and then click the **Virtual Power** button. This will immediately remove power from the system. The system will restart after approximately six seconds. This option is not displayed when the server is off.

**NOTE:** Using this option will circumvent any graceful shutdown features of the operating system.

- **Cold Boot of system**—This option turns the server off, then back on.
- **Warm Boot of system**—This option causes the server to reset, without turning it off. To use this option, selecting **Warm Boot of system** and click the **Virtual Power** button. This option is not displayed when the server is off.

**NOTE:** Using this option will circumvent any graceful shutdown features of the operating system.

- **Automatically Power On Server**—This option automatically turns the server on when AC power is applied, if **Yes** is selected. AC power is applied when the server is plugged in or when a UPS is activated after a power outage. The server automatically powers on and begins the normal server booting process.
- **Manual Override for BL p-Class**—This option is displayed only when you are connected to a ProLiant BL p-Class server. This option enables you to forcibly power on a server, even if the rack reports insufficient power. An improperly configured rack or rack communication problem may cause a server to not power on when sufficient power is available. This option should only be used if you are certain your rack has sufficient power capacity.



**CAUTION:** It is possible using the **Manual Override for BL p-Class** option to power on servers that exceed the power available from the power supplies. Exceeding the available power can cause loss of all servers in the rack, server failures, and loss or corruption of data. HP recommends correcting configuration or communication problems to ensure reliable operation.

## Virtual Media

Virtual Media is advanced functionality enabled by licensing the optional iLO Advanced Pack. If not licensed, the message iLO feature not licensed is displayed.

The iLO **Virtual Media** option provides the administrator with a Virtual Floppy disk drive and a Virtual CD drive. The iLO Virtual Media devices connect to the host server using USB technology. The iLO Virtual Media devices are available when the host system is booting. Using USB also enables new capabilities for the iLO Virtual Media devices when connected to USB-supported operating systems. The iLO Virtual Media devices are available to the host operating system, on USB-supported operating systems, without any additional HP drivers running on the server.

Different operating systems provide varying levels of USB support. The iLO Virtual Media is configurable to address these varying levels of support ("Operating System USB Support" on page 53).

## Operating System USB Support

The different operating systems provide varying levels of USB support. iLO uses the built-in USB drivers of the operating system. The level of support for iLO Virtual Media is affected by the level of USB support in the operating system. In general, any operating system issues that affect a physical USB floppy drive will also impact the iLO Virtual Media.

Support at server boot time for Virtual Floppy is provided by the HP server ROM. The Virtual Floppy will be available at boot time regardless of the server operating system.

The following server operating systems do not support USB media and, therefore, do not have access to Virtual Floppy during operating system run time:

- Microsoft® Windows NT® 4.0
- Linux Red Hat (before 7.2)
- SuSE Linux (before 7.0)
- Novell NetWare 5.x and 6

Certain Linux operating systems do not correctly support USB Virtual Floppy drives at operating system install time. The iLO Virtual Media should not be used during the installation of the following Linux operating systems:

- Linux Red Hat 7.2 Professional
- SuSE Linux 7.0

Windows® 95 OSR 1 does not support any USB devices. Therefore, SmartStart 5.x CDs cannot be used with the iLO Virtual Media.

The table below lists operating system USB capabilities and the corresponding iLO Virtual Media capabilities.

	<b>NetWare</b>	<b>SuSE (before 7.0)</b>	<b>Red Hat (before 7.2)</b>	<b>Red Hat 7.2 SuSE 7.0</b>	<b>Windows NT®</b>	<b>Windows® 2000</b>	<b>Windows® Server 2003</b>
Pre-operating system server boot USB floppy	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Operating system install using USB floppy	No	No	No	No	No	Yes	Yes
Operating system install using USB CD	No	No	No	No	No	Yes	Yes
Operating system run time using USB floppy	No, Yes for NW6.5	No	No	Yes	No	Yes	Yes

## Using iLO Virtual Media Devices

To use the iLO Virtual Media devices, select the **Virtual Media** option on the **Virtual Devices** tab. An applet loads in support of the virtual floppy or virtual CD-ROM device.

There are four modes supported by the Virtual Media applet. The desired operating mode is selected by clicking the **Configure** button in the Virtual Media applet. The four modes are

- Floppy only—In this mode, only the virtual floppy disk is available.
- CD-ROM only—In this mode, only the virtual CD-ROM disk is available.
- Automatic—In the Automatic mode, the device that is selected last is the device that is available. Only one of the devices (Virtual Floppy or Virtual CD) can be selected at any one time.
- Composite—In the composite mode, either one or both of the devices can be selected. If both devices are selected, then both devices are available at the same time. In composite mode, neither CD-ROM or floppy are available for use locally on the client machine. Not all operating systems support the composite mode.
  - Bios and DOS® support composite mode.
  - Windows® 2000, Windows® 2000 with SP1,SP2 do not support composite mode for mass storage devices. Any composite device configuration that includes a mass storage device will result in an unavailable mass storage device.
  - Windows® 2000 with SP3 supports composite mode.
  - Windows® Server 2003 supports composite mode.
  - Linux supports composite mode, with the exception of multiple mass storage devices in your composite device. A composite device consisting of multiple mass storage devices will have disconnect and reconnect problems. Composite mode supports composite devices such as a keyboard, mouse and floppy.

## iLO Virtual Floppy

The iLO Virtual Floppy disk is available at server boot time for all operating systems. Booting from the iLO Virtual Floppy allows you to upgrade the host system ROM, deploy an operating system from network drives, and perform disaster recovery of failed operating systems, among other tasks.

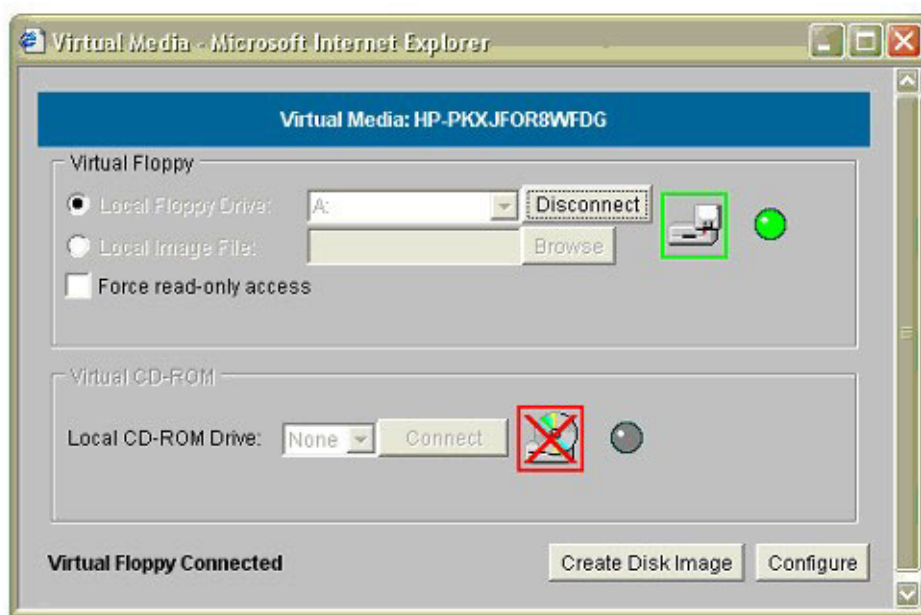
If the host server operating system supports USB mass storage devices, then the iLO Virtual Floppy will also be available after the host server operating system loads. You can use the iLO Virtual Floppy when the host server operating system is running to upgrade device drivers, create an emergency repair diskette, and perform other tasks. Having the Virtual Floppy available when the server is running can be especially useful if the administrator needs to diagnose and repair a problem with the network interface controller driver.

The Virtual Device can be the physical floppy drive where you are running the Web browser, or an image file stored on your local hard drive or network drive. For maximum performance, HP recommends the use of local image files stored either on the hard drive of your Client PC or on a network drive accessible through a high-speed network link.

To use a physical floppy drive in your client PC:

1. Select **Local Floppy Drive**.
2. Select the drive letter of the desired physical floppy drive on your client PC from the dropdown menu.

3. Click **Connect**.



To use an image file:

1. Select **Local Image File** within the Virtual Floppy section of the **Virtual Media** applet.
2. Enter the name of the diskette image in the text box. You can also use **Browse** to locate image files.
3. Click **Connect**.

When connected, the Virtual Devices will be available to the host server until you close the **Virtual Media** applet. When you are finished using the Virtual Floppy, you can either select to disconnect the device from the host server or close the applet.

**NOTE:** The **Virtual Media** applet must remain open in your browser as long as you continue to use a Virtual Media Device.

The iLO Virtual Media floppy will be available to the host server at run time if the operating system on the host server supports USB floppy drives. Windows® 2000 and Linux operating systems support USB floppy drives at the time of the publication of this manual.

The iLO Virtual Floppy appears to your operating system just like another floppy as shown. This example displays iLO using a Virtual Floppy connected as B.

**NOTE:** The host operating system may prompt you to complete a New Hardware Found wizard the first time you use the iLO Virtual Media feature.

**NOTE:** You might receive a warning message from the host operating system regarding unsafe removal of a device when you disconnect from the iLO Virtual Media feature. This warning can be avoided by using the operating system-provided feature to stop the device before disconnecting it from the Virtual Media.

## Creating an iLO Virtual Floppy Image

The iLO Virtual Media feature enables you to create floppy image files within the same applet. You can create image files from diskettes and create diskettes from existing image files. The performance of iLO Virtual Floppy is faster when image files are used.

To create a Virtual Media image file:

1. Click **Create Disk Image**.
2. Select the drive letter and the image file name. You can use the **Browse** feature to find and select an existing image file or to change the directory in which the image file will be created.
3. Click **Create**. The Virtual Media applet begins the process of creating the image file. The process is complete when the progress bar reaches 100 percent.

**Disk >> Image** changes to **Image >> Disk** when clicked. Use this button to switch from creating image files from physical diskettes to creating physical floppy diskettes from image files.



## Mounting a USB Virtual Media Floppy in Linux

1. Access iLO through a browser.
2. Click **Virtual Media** in the **Virtual Devices** tab.
3. Select a diskette drive or diskette image to be used and click **Connect**.
4. Load the USB drivers, using the following commands:

```
modprobe usbcore  
modprobe usb-storage  
modprobe usb-ohci
```

5. Load the SCSI disk driver, using the following command:

```
modprobe sd_mod
```

6. Mount the floppy drive, using the following command:

```
mount /dev/sda /mnt/floppy -t vfat
```

**NOTE:** Use the man mount command for additional file system types.

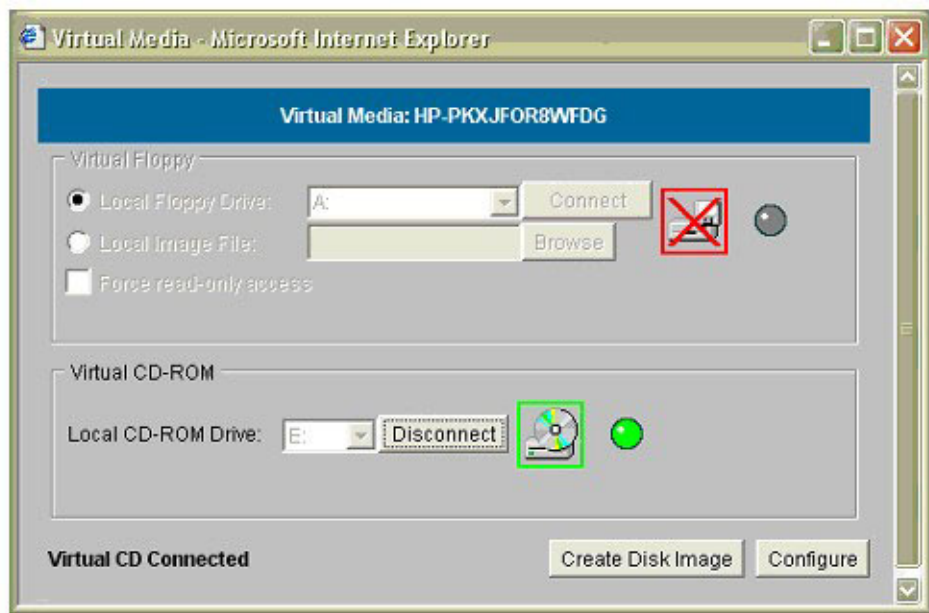
## iLO Virtual CD-ROM

To use the iLO Virtual CD, select the **Virtual Media** option on the **Virtual Devices** tab. An applet loads the Virtual CD device.

To use a physical floppy drive in your client PC:

1. Select **Local CD-ROM Drive**.
2. Select the drive letter of the desired physical CD-ROM drive on your client PC from the dropdown menu.

3. Click **Connect**.



### Mounting a USB Virtual Media CD\_ROM in Linux

1. Access iLO through a browser.
2. Click **Virtual Media** in the **Virtual Devices** tab.
3. Select a CD-ROM to be used and click **Connect**.
4. Load the USB drivers using the following commands:  

```
modprobe usbcore  
modprobe usb-storage  
modprobe usb-ohci
```
5. Load the SCSI CD-ROM disk driver using the following command:  

```
modprobe sr_mod
```
6. Mount the floppy drive using the following command:  

```
mount /dev/scd0 /mnt/cdrom -t iso9660
```

**NOTE:** Use the `man mount` command for additional file system types.

## Virtual Media Applet Time-out

The Virtual Media applet does not have a time-out when Virtual Media is connected to the host server. Even when the user logs out, the Virtual Media applet will maintain the connection so the host server has access to the Virtual Media. However, the Virtual Media applet does have a timeout when Virtual Media is not connected. If you are starting the Virtual Media applet without connecting Virtual Media to the host server or disconnecting Virtual Media after using the applet, there is a limited time to reconnect before the Virtual Media applet closes. The timeout value is the same as the value set in the **Idle Connection Timeout (minutes)** field on the **Global Settings** screen. When the Idle Connection Timeout occurs, the user will be logged out and the Virtual Media applet will be closed unless Virtual Media is connected.

## iLO Virtual Media Privilege

The ability to use the iLO Virtual Media is restricted by an iLO User Privilege. Authorized users must have the Virtual Media privilege to select a Virtual Media Device and connect it to the host server.

**IMPORTANT:** Do not attempt to upgrade the iLO firmware from a ROMPaq diskette using the iLO Virtual Floppy. The preferred method of remotely upgrading the iLO firmware is to use the **Upgrade iLO Firmware** option on the **Administration** tab.

## Virtual Serial Port

The Virtual Serial Port provides a Java™ applet that allows connection to the server serial port. The Java™ applet provides VT320 terminal emulation to access an application configured for the serial port.

## Windows EMS Console

A feature of Windows® Server 2003 is the EMS. The typical usage model for the EMS console is to physically connect a serial cable to the server. iLO, however, enables you to use EMS over the network through a Web browser. Microsoft® EMS gives you the ability to display running processes, change the priority of processes, and halt processes. The EMS console and the iLO Remote Console may be used at the same time.

The Windows® EMS Console, if enabled, provides the ability to perform EMS in cases where video, device drivers, or other operating system features have prevented normal operation and normal corrective actions from being performed.

The Windows® EMS serial port must be enabled through the host system RBSU. The configuration allows for the enabling or disabling of the EMS port, and allows for the selection of the COM port. The iLO system will automatically detect whether the EMS port is enabled or disabled, and the selection of the COM port.

To obtain the `SAC>` prompt, typing `enter` may be required after connecting through the Virtual Serial Port console.

For more information on using the EMS features, refer to the Windows® Server 2003 Server documentation.

## **Security Information**

If Remote Console Data Configuration is enabled, the Virtual Serial Port data stream is encrypted as data is passed between the iLO system and the viewing applet.

## **Virtual Indicators**

iLO provides the ability to monitor and control the status of the Unit ID LED. The Unit ID LED is the blue LED on the HP server that is used for identifying systems in a rack full of servers. iLO enables you to view the status of the Unit ID LED and change the status using iLO Web pages.

The Unit ID LED also blinks whenever a critical Remote Management task is currently active on the server. A blinking Unit ID LED indicates that the server is in the midst of an activity that you should not interrupt. Never remove power from a server with a blinking Unit ID LED.

The Unit ID LED will blink while the server is under active iLO Remote Console control, while iLO settings are being modified through XML scripting, while the iLO firmware is being updated.

## Administration

The options available in the **Administration** tab enable you to manage user settings, SNMP alerting through integration with Insight Manager 7, security settings, and network environment settings. This section also provides a firmware upgrade option that allows you to keep iLO current.

## User Administration

**User Administration** enables you to manage the user accounts stored locally in the secure iLO memory. Directory user accounts are managed using MMC or ConsoleOne snap-ins. Using the **User Administration** screen, you can add a new user, view or modify an existing user's settings, or delete a user.

**NOTE:** To align common directory server architecture on all Lights-Out Management devices, version 1.40 of the iLO firmware has different user privileges from previous versions of the firmware.

### Adding a New User

**IMPORTANT:** Only users with the Administer User Accounts privilege can manage other users on iLO.

You can assign a different access privilege to each user. Each user can have a unique set of privileges, designed for the tasks that the user must perform. Access to critical functions, such as Remote Console, Managing Users, Virtual Power Button, and other features can be denied.

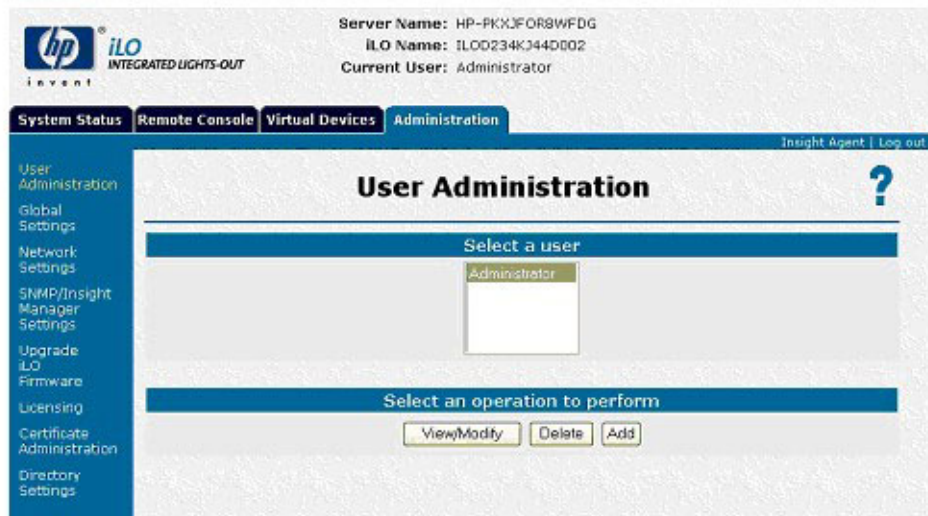
iLO supports the configuration of up to 12 users. Login attempts are tracked and login failures are logged. You have the option of generating alerts on a remote management PC running Insight Manager 7 when login attempts fail. iLO supports all LAN-oriented security features and dynamic password encryption.

To support more than 12 users, iLO Advanced 1.40 and later allows integration with directory-based user accounts. This enables virtually unlimited user accounts.

To add a new user to iLO:

1. Log on to iLO using an account that has the Administer User Accounts privilege. Click **Administration**.

- Click **User Administration**. A screen similar to the one shown is displayed.



- Click **Add**.
- Complete the fields with the necessary information for the user being added.
- When the user profile is complete, click **Save User Information** to return to the **User Administration** screen. To clear the user profile form while entering a new user, click **Restore User Information**.

## Viewing or Modifying an Existing User's Settings

**IMPORTANT:** Only users with the Administer User Accounts privilege can manage other users on iLO. All users may change their own password using the **View/Modify User** feature.

To view or modify an existing user's information:

- Log on to iLO using an account that has the Administer User Accounts privilege. Click **Administration**.
- Click **User Administration** and select from the list the name of the user whose information you want to change.
- Click **View/Modify User**.

4. Change the user information in the fields that require modification. After changing the fields, click **Save User Information** to return to the **User Administration** screen. To recover the user's original information, click **Restore User Information**. All changes made to the profile will be discarded.

## Deleting a User

**IMPORTANT:** Only users with the Administer User Accounts privilege can manage other users on iLO.

To delete an existing user's information:

1. Log on to iLO using an account that has the Administer User Accounts privilege. Click **Administration**.
2. Click **User Administration** and select from the list the name of the user whose information you want to change.
3. Click **Delete User**. A pop-up window is displayed stating, Are you sure you want to delete the selected user? Click **OK**.

## Network Settings

The **Network Settings** option enables you to view and modify the NIC IP address, subnet mask, and other TCP/IP-related settings. From this screen you can enable or disable DHCP and, for servers not using DHCP, you can configure a static IP address.

To change network settings for iLO:

1. Log on to iLO using an account that has the Configure iLO Settings privilege. Click **Administration**.  
**IMPORTANT:** These settings can be changed only by users with the Configure iLO Settings privilege. Users that do not have the Configure iLO Settings privilege will only be able to view the assigned settings.
2. Click **Network Settings**.

3. Change the network settings as needed by entering your selections in the fields. After the parameter ("Network Settings Parameters" on page 216) changes have been made, click **Apply** to complete the changes.

hp iLO INTEGRATED LIGHTS-OUT

Server Name: HP-PK0JFOR8WFDG  
iLO Name: ILO0234KJ44D002  
Current User: Administrator

System Status Remote Console Virtual Devices Administration

Insight Agent | Log out

## Network Settings

### Standard Configuration Parameters

Enable NIC: ☒ Yes ☐ No

Transceiver Speed Autoselect: ☒ Yes ☐ No

Speed: ☒ 10 MBits/s ☐ 100 MBits/s ☐ 1000 MBits/s

Duplex: ☒ Half ☐ Full

Enable DHCP: ☒ Yes ☐ No

Use DHCP Supplied Gateway: ☒ Yes ☐ No

Use DHCP Supplied DNS Servers: ☒ Yes ☐ No

Use DHCP Supplied WINS Servers: ☒ Yes ☐ No

Use DHCP Supplied Static Routes: ☒ Yes ☐ No

Use DHCP Supplied Domain Name: ☒ Yes ☐ No

Register With WINS Server: ☒ Yes ☐ No

Register With DDNS Server: ☒ Yes ☐ No

Ping Gateway on Startup: ☐ Yes ☒ No

IP Address: 16.100.241.130

Subnet Mask: 255.255.252.0

Gateway IP Address: 16.100.240.1

### Advanced Configuration Parameters

iLO Subsystem Name: ILO0234KJ44D002

Domain Name: americas.cpqcorp.net

DHCP Server: 16.110.251.250

Primary DNS Server: 16.110.251.242

Secondary DNS Server: 16.110.251.243

Tertiary DNS Server: 16.103.131.242

When you click **Apply**, iLO restarts, and the connection of your browser to iLO terminates. To reestablish a connection, wait 60 seconds before launching another Web browser session and logging in.



## iLO Diagnostic Port Configuration Parameters

The iLO Diagnostic Port on the front of ProLiant BL p-Class servers enables you to access and troubleshoot server issues by using a diagnostic cable. The iLO Diagnostic Port uses a static IP address. It does not use DHCP to obtain an IP address, register with WINS or dynamic DNS, or use a gateway. The diagnostic port cable should not be left plugged in without an active network connection, as it will cause degraded network performance on the standard iLO network port.

In **Network Settings**, you can configure specific diagnostic port information. For more information on using the diagnostic port and the diagnostic cable, refer to the Setup and Installation Guide for the blade server.

The following are the fields that can be configured for the diagnostic port:

**NOTE:** The availability of the diagnostic port is controlled by the **Enable NIC** field. If **Enable NIC** is set to **Yes**, the diagnostic port is enabled.

### Transceiver Speed Autoselect

Autoselect detects the interface speed and sets the interface to operate at 10 Mbps or 100 Mbps and at half or full duplex. If necessary, this parameter can be set to manual to allow manual adjustment of speed and duplex settings.

#### Speed

Use this setting to assign 10-Mbps or 100-Mbps connect speeds if Transceiver Speed Autoselect is not enabled.

#### Duplex

Use this setting to assign half or full duplex to the NIC if Transceiver Speed Autoselect is not enabled.

#### IP Address

Use this parameter to assign a static IP address on your network to the iLO Diagnostic Port. By default, the IP address is 192.168.1.1 for all iLO Diagnostic Ports.

### **Subnet Mask**

Use the subnet mask parameter to assign the subnet mask for the iLO Diagnostic Port. By default, the subnet mask is 255.255.255.0 for all iLO Diagnostic Ports.

The use of the diagnostic port is automatically sensed when an active network cable is plugged into it. When switching between the diagnostic and back ports, you must allow 90 seconds for the network switchover to complete before attempting connection through the Web browser.

**NOTE:** The diagnostic port will not switchover if there is an active Remote Console session or a firmware update in progress.

## **Global Settings**

The **Global Settings** option enables you to view and modify security settings for iLO. This screen enables you to configure the Remote Console timeout, as well as the iLO ports to be used for the iLO Web Server, Remote Console, and Virtual Media. These settings are applied globally, regardless of the individual user settings.

**IMPORTANT:** These settings can be changed only by users with the Configure iLO Settings privilege. Users that do not have the Configure iLO Settings privilege will only be able to view the assigned settings.

The screenshot displays the HP iLO web interface. At the top, the server name is HP-PK0JFOR8WFDG and the iLO name is ILOD234KJ44D002. The user is Administrator. The navigation bar includes System Status, Remote Console, Virtual Devices, and Administration. The left sidebar lists various administration tasks. The main content area is titled 'Global Settings' and contains a 'Security Settings' section with the following options:

- Idle Connection Timeout (minutes): 15
- Enable Lights-Out Functionality: ☒ Yes ☐ No
- Enable iLO ROM-Based Setup Utility: ☒ Yes ☐ No
- Require Login for iLO RBSU: ☐ Yes ☒ No
- Remote Console Port Configuration: ☐ Enabled ☐ Disabled ☒ Automatic
- Remote Console Data Encryption: ☐ Yes ☒ No
- SSL Encryption Strength: 128-bit
- Current Cipher: RC4-MD5 with 128 bit encryption
- Web Server Non-SSL Port: 80
- Web Server SSL Port: 443
- Virtual Media Port: 17988
- Remote Console Port: 23
- Minimum Password Length: 0

A note at the bottom states: "NOTE: The Integrated Lights-Out subsystem must be restarted before any port changes you make on this screen will take effect. Pressing the Apply button below terminates your browser connection and restarts Integrated Lights-Out if any changes have been made to port settings. In this case you must wait at least 30 seconds before attempting to reestablish a connection with Integrated Lights-Out." An 'Apply' button is located at the bottom right of the settings area.

The **Global Settings** option enables you to define the following functions:

### Idle Connection Timeout (Minutes)

This option specifies the interval of user inactivity, in minutes, before the Web server and Remote Console session are automatically terminated.

### Enable Lights-Out Functionality

This option allows connection to iLO. If disabled, all connections to iLO are prevented. The default setting is **Yes**.

- The iLO 10/100 network and communications with operating system drivers will be turned off if Lights-Out functionality is disabled. The iLO Diagnostic Port for a ProLiant BL p-Class server will be disabled as well.
- If iLO functionality, including the iLO Diagnostic Port, is disabled, you must use the Security Override Switch in the server to enable iLO functionality. Follow the documentation of the server to locate the Security Override Switch and set it to the override position. Power on the server and use the iLO RBSU to set **Enable Lights-Out Functionality**.

### **Enable iLO ROM-Based Setup Utility**

This option enables a user with access (physical or virtual) to the host to configure iLO for that system using the iLO RBSU. RBSU is invoked when the host system reboots and performs POST. The default setting is Yes. You can restrict RBSU access to authorized users using the **Require Login for iLO RBSU** setting.

**NOTE:** If the physical security jumper is set, the RBSU prompt displays during reboot.

### **Require Login for iLO RBSU**

This option specifies whether the user is required to provide a login name and password to access the iLO RBSU. The default setting is No.

### **Remote Console Port Configuration**

This option enables or disables configuring of the port address. Setting this option to **Enabled** allows Telnet and Remote Console applet access. Setting this option to **Disabled** turns off both Telnet and Remote Console applet access.

**Remote Console Data Encryption** must be set to **No** to use Telnet to access the text Remote Console.

### **Remote Console Data Encryption**

This option enables encryption of Remote Console data. If using a standard Telnet client to access the iLO, this setting must be set to **No**.

### **SSL Encryption Strength**

---

This option displays the current cipher strength setting. The most secure is 128-bit (High).

### **Current Cipher**

This option displays the encryption algorithm currently being used to protect data during transmission between the browser and the iLO.

### **Web Server Non-SSL Port**

The embedded Web server in iLO is configured by default to use port 80 for unencrypted communications. This port setting is configurable in the **Global Settings** option of the **Administration** tab.

### **Web Server SSL Port**

The embedded Web server in iLO is configured by default to use port 443 for encrypted communications. This port setting is configurable in the **Global Settings** option of the **Administration** tab.

### **Virtual Media Port**

The Virtual Media support in iLO uses a configurable port for its communications. This port can be set in the **Global Settings** option of the **Administration** tab. The default setting is to use port 17988.

### **Remote Console Port**

The iLO Remote Console is configured by default to use port 23 for Remote Console communications. This port setting is configurable in the **Global Settings** option of the **Administration** tab.

### **Minimum Password Length**

This option specifies the minimum number of characters allowed when a user password is set or changed. The character length can be set at a value from 0 to 39. The default setting is eight characters.

## SNMP/Insight Manager Settings

The **SNMP/Insight Manager Settings** option enables you to configure SNMP alerts, generate a test alert, and configure integration with Insight Manager 7.

### Enabling SNMP Alerts

iLO supports up to three TCP/IP addresses to receive SNMP alerts. Typically, this address is the same as the TCP/IP address of the Insight Manager 7 server console.

**IMPORTANT:** These settings can be changed only by users with the Configure iLO Settings privilege. Users that do not have the Configure iLO Settings privilege will only be able to view the assigned settings.

Two alert options are available in the **SNMP/Insight Manager Settings** screen:

- **Enable iLO SNMP Alerts**—The SNMP alerts are generated by iLO and are independent of the host server operating system. Alerts include major events, such as host server power outage or host server reset, and iLO events such as an unauthorized login attempt. These alerts take the form of an Insight Manager SNMP trap.
- **Forward Insight Manager Agent SNMP Alerts**—The Insight Management agents provided for each supported network operating system to generate these alerts. These agents also must be installed on the host server to receive these alerts. iLO forwards the alerts to Insight Manager 7.

To configure alerts:

1. Log on to iLO using an account that has the Configure iLO Settings privilege.

2. Click **SNMP/Insight Manager Settings** in the **Administration** tab. A screen similar to is displayed.

The screenshot shows the iLO Administration interface. At the top, the HP iLO logo is on the left, and server information is on the right: Server Name: HP-PK0JF0R8WFDG, iLO Name: ILOD234K344DD02, Current User: Administrator. Below this is a navigation bar with tabs: System Status, Remote Console, Virtual Devices, and Administration (selected). On the left is a vertical menu with options: User Administration, Global Settings, Network Settings, SNMP/Insight Manager Settings (selected), Upgrade iLO Firmware, Licensing, Certificate Administration, and Directory Settings. The main content area is titled 'SNMP/Insight Manager Settings' with a help icon (?). It contains two sections: 'Configure and Test SNMP Alerts' and 'Configure Insight Manager Integration'. The first section has a text field for 'SNMP Alert Destination(s):', radio buttons for 'Enable iLO SNMP Alerts' (Yes/No) and 'Forward Insight Manager Agent SNMP Alerts' (Yes/No), and a 'Send Test Alert' button. The second section has a text field for 'Insight Manager Web Agent URL:' followed by ':2301', a dropdown for 'Level of Data Returned' set to 'Medium (iLO+Server Association Data)', a 'View XML Reply' link, and 'Apply Settings' and 'Reset Settings' buttons.

3. Enter up to three TCP/IP addresses to receive the SNMP alerts.
4. Select the alert options you want iLO to support.
5. Click **Apply Settings**.

## Generating Test Alerts

Test alerts are generated by means of the **SNMP/Insight Manager Settings** in the **Administration** section of the iLO navigation frame. These alerts include an Insight Manager SNMP trap and are used to verify the network connectivity of iLO in Insight Manager 7. Only users with the Configure iLO Settings privilege can send test alerts.

Click **Apply Settings** to save any changes made to **SNMP Alert Destination(s)** before sending a test alert.

To send a test alert:

1. Click **SNMP/Insight Manager Settings** in the **Administration** tab.

2. Click **Send Test Alert** to generate a test alert and send it to the TCP/IP addresses saved in the **SNMP Alert Destination(s)** fields.
3. After generating the alert, a confirmation screen is displayed.
4. Check the Insight Manager 7 console for receipt of the trap.

## Insight Manager 7 Integration

iLO enables you to configure the URL (DNS name or IP address) of the Insight Manager Web Agents running on the host server. You may also configure the level of data returned with Insight Manager 7 identification information.

The **Insight Manager Web Agent URL** field enables you to enter the IP address or the DNS name of the host server on which the Insight Manager Web Agents are running. Entering this data in the field provided enables iLO to create a link from the iLO Web pages to the pages of the Web Agent.

**NOTE:** The expected entry in the **Insight Manager Web Agent URL** field is the IP address or the DNS name only. The protocol (for example, "http://") and a port ID (for example, ":2301") should not be entered.

The link to the Insight Web Agents is found on the blue header bar, next to the **Log out** link.

The **Level of Data Returned** field enables you to control the amount of information that is returned to Insight Manager 7. This information is used to associate management processors with servers and is displayed on the summary page for iLO in Insight Manager 7.

## Upgrade iLO Firmware

Firmware upgrades enhance the functionality of iLO. The firmware upgrade can be done from any network client using a standard Web browser. Only users with the Update iLO Firmware privilege can upgrade the iLO firmware. The most recent firmware for iLO is available on the HP website. To upgrade the iLO firmware using a standard Web browser:

1. Log on to iLO using an account that has the Update iLO Firmware privilege.



- Click **Upgrade iLO Firmware** in the **Administration** tab. A screen similar to is displayed.

The screenshot shows the HP iLO Integrated Lights-Out Administration web interface. At the top, the HP iLO logo is on the left, and server information is on the right: Server Name: HP-PKXJFOR8WFDG, iLO Name: iLOD234KJ44D002, and Current User: Administrator. Below this is a navigation bar with tabs: System Status, Remote Console, Virtual Devices, and Administration (which is selected). On the far right of the navigation bar is a link for 'Insight Agent | Log out'. A left-hand sidebar contains a list of links: User Administration, Global Settings, Network Settings, SNMP/Insight Manager Settings, Upgrade iLO Firmware (which is highlighted), Licensing, Certificate Administration, and Directory Settings. The main content area is titled 'Upgrade iLO Firmware' with a question mark icon. It is divided into two sections. The first section, 'Current Firmware Status', shows 'Firmware Revision: 1.40' and 'Firmware Date: 03/29/2003'. The second section, 'Select New Firmware Image', contains a text field labeled 'New firmware image', a 'Browse...' button, and a 'Send firmware image' button. A note at the bottom states: 'Note: Do not power cycle, click on another link, or otherwise interrupt the firmware upgrade while it is in progress. While the Integrated Lights-Out system is being updated, it will appear to be unavailable if you attempt to view it with Insight Manager.'

- Enter the file name in the **New firmware image** field or **Browse** for the file. Click **Send firmware image**.
- The firmware upgrade takes a couple of minutes. A progress bar displays the progress of the firmware upgrade.

**IMPORTANT:** Do not interrupt an Upgrade iLO Firmware session that is in progress.

The iLO system automatically resets at the end of a successful firmware upgrade. The host operating system and server are not affected by the iLO system being reset.



**WARNING:** After upgrading to version 1.40, a subsequent downgrade to any previous version may result in loss of configuration data. Before downgrading from firmware version 1.40 to any other version, HP recommends that you back up your configuration data.

If the firmware upgrade was interrupted or failed, immediately attempt the upgrade again. Do not reset the iLO system before reattempting a firmware upgrade. iLO provides an FTP-based firmware upgrade disaster recovery ("Inability to Upgrade iLO Firmware" on page 239) if a firmware upgrade is interrupted or failed.

**NOTE:** For systems with diskette drives, you can also update the iLO firmware using ROMPaq diskettes. HP does **not** recommend updating iLO firmware using the Virtual Media floppy diskette.

## Licensing

The iLO Advanced License Activation page is used to apply the license activation for the iLO Advanced Pack. The "Enabling iLO Advanced Functionality (on page 18)" section discusses the steps required to enter the activation key and enable the advanced features.

## Certificate Administration

**Certificate Information** displays the information associated with the stored certificate. Information is encoded in the certificate by the CA, and is extracted by iLO for display.

- **Issued To** is the entity to whom the certificate was issued.
- **Issued By** is the CA which issued the certificate.
- **Valid From** is the date from which the certificate is valid.
- **Valid Until** is the date which the certificate will expire.
- **Serial Number** is the serial number assigned to the certificate by the CA.

**Importing a Certificate** displays information on how to import a certificate. For more information on importing certificates, refer to "Certificates (on page 97)" in the "Security for Integrated Lights-Out (on page 93)" section.

## Directory Settings

The Directory Settings screen enables you to configure and test your directory services. For additional information on directories, refer to the "Directory Services (on page 99)" section. For additional information on directory configuration parameters, refer to the "Configuring Directory Settings (on page 135)" section.

## ProLiant BL p-Class

The **BL p-Class** tab enables you to control specific settings for the ProLiant BL p-Class blade server rack. iLO also provides Web-based diagnostics for the ProLiant BL p-Class server rack. These diagnostics are listed on four Web pages under the **BL p-Class** tab.

**NOTE:** The fourth Web page is available when there is a redundant power management module in the server configuration.

## Rack Settings

Blade servers communicate with the rack environment to obtain power and manage shared resources of the rack (fans, temperature, power supplies). The **Rack Settings** option allows you to configure this communication.

hp iLO INTEGRATED LIGHTS-OUT

Server Name: Administration  
iLO Name: iLOB119JTN8085E  
Logged in: Administrator

System Status Remote Console Virtual Devices Administration **BL p-Class** Insight Agent | Log out

Rack Settings  
Rack Topology  
Server Blade Mgt. Module  
Power Mgt. Module  
Redundant Power Mgt. Module

## Rack Settings

### Rack Information

Rack Name	North America	Rack Serial Number	2098DWA94E1
Enclosure Name	Accounting	Enclosure Serial Number	DY1962W40E88
Bay Name	Accounts Payable	Blade Serial Number	68D01YE10062

Bay 8

### Power On Control

Power Source: ☒ Rack Provides Power ☐ Facility Provides 48V

Enable Automatic Power On: ☒ Yes ☐ No

Enable Rack Alert Logging (IML): ☒ Yes ☐ No

Apply

The following fields are available:

### Rack Name

The rack name is used to logically group together the components that comprise a single rack. When changed, the rack name is communicated to all other components connected in a rack. The name is used when logging and alerting to assist in identifying the component.

### Enclosure Name

The enclosure name is used to logically group together the server blades that comprise a single enclosure. When changed, the enclosure name is communicated to all other server blades connected in the same enclosure. The name is used when logging and alerting to assist in identifying the component.

### Bay Name

The bay name is used when logging and alerting to assist in identifying a component or its function.

### Bay

The ProLiant BL p-Class enclosure can support one to eight server blades. The bays are numbered from left to right starting with 1 and finishing with 8. The bay number is used to assist in physically identifying the faulty server blade or other error conditions. This information is for viewing only.

### **Rack Serial Number**

The rack serial number identifies the components in the rack as a logical grouping. The serial number is determined during power-up of the various components to create a unique rack serial number. Switching components (server blade enclosure or power supplies) alters the rack serial number.

### **Enclosure Serial Number**

The enclosure serial number identifies the particular server blade enclosure in which a server blade resides.

### **Blade Serial Number**

The blade serial number identifies the serial number for the server blade product.

### **Power Source**

The server blade enclosure can be installed in a rack by using one of two configurations:

- The server blade power supplies can be used to convert normal AC facility power to 48 V DC to power the rack. In this configuration, select the power source as **Rack Provides Power**. This setting allows each server blade, enclosure, and power supply to communicate power requirements to ensure proper power consumption without risking power failures.
- If the facility can provide 48 V DC power directly, without the need for the provided power supplies, then select **Facility Provides 48V**. Each server blade will not be required to communicate with the infrastructure for power when powering on or off.

**NOTE:** It is essential that proper power sizing requirements be performed to ensure sufficient power for all the server blades and other components of the rack.

### **Enable Automatic Power On**

Each server blade can be configured to automatically power on when inserted into the enclosure. Depending on the Power Source setting, the server blade communicates with the rack to determine if enough power is available to power on. If the power is available, then the server blade automatically powers on and begins the normal server booting process.

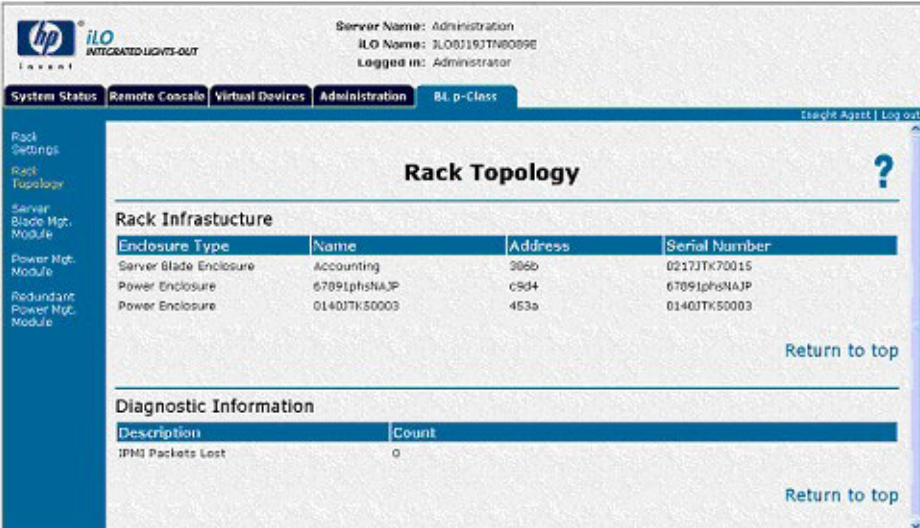
### Enable Rack Alert Logging

As the server blade receives alerts, these events can be logged to the IML. You can view these events by using the **iLO System Status—IML** tab. Additional IML viewing tools are available to allow viewing from the installed operating system on the server blade.

## Rack Topology

The **Rack Topology** screen:

- Discovers all devices connected in the rack.
- Displays the enclosure type, name, address, and serial number.
- Displays diagnostic information for the rack.



The screenshot displays the HP iLO Rack Topology interface. At the top, it shows the HP iLO logo and the text 'INTEGRATED LIGHTS-OUT'. The user is logged in as 'Administrator' with the iLO Name 'ILOB119JTNB089E'. The interface has a navigation bar with tabs: System Status, Remote Console, Virtual Devices, Administration, and BL p-Class. The 'Administration' tab is selected, and the 'Rack Topology' screen is displayed. The screen title is 'Rack Topology' with a help icon. Below the title, there is a section for 'Rack Infrastructure' with a table listing enclosure types, names, addresses, and serial numbers. A 'Return to top' link is present. Below this, there is a 'Diagnostic Information' section with a table showing the count of IPMI Packets Lost. Another 'Return to top' link is at the bottom right.

Enclosure Type	Name	Address	Serial Number
Server Blade Enclosure	Accounting	386b	0217JTK70015
Power Enclosure	67891phsNAJP	c9d4	67891phsNAJP
Power Enclosure	0140JTK50003	453a	0140JTK50003

Description	Count
IPMI Packets Lost	0

## Server Blade Management Module

The **Server Blade Management Module** screen:

- Displays devices discovered in the BL p-Class enclosure.
- Reads and displays the current firmware version of the controller for the blade server enclosure.
- Detects and displays the fuse state and power state of blade servers.
- Allows you to activate the enclosure LEDs.

hp iLO INTEGRATED LIGHTS-OUT  
Server Name: Administration  
iLO Name: iLO0319JTN0089E  
Logged in: Administrator

System Status Remote Console Virtual Devices Administration BL p-Class

### Server Blade Management Module

Enclosure Information

Name	Serial Number	Temp (°C)	FW Rev	HW Rev
Accounting	DY1962W40E08	32	0.92	4

[Return to top](#)

Server Component Information

Bay Number	Occupied	Fuse A	Fuse B	Power
1	Empty	Good	Open	Unknown
2	Empty	Good	Open	Unknown
3	Empty	Good	Open	Unknown
4	Empty	Good	Open	Unknown
5	Present	Good	Open	Unknown
6	Present	Good	Open	Unknown
7	Present	Good	Open	Unknown
8	Present	Good	Open	On

[Return to top](#)

## Power Management Module

The **Power Management Module** screen:

- Detects and displays the main power supplies.
- Reads and displays the current firmware version of the controller for the power supply enclosure.
- Displays the current power output, maximum power output, and temperature information for the power supply.

- Allows you to activate the power management module LEDs.

The screenshot displays the HP iLO Integrated Lights-Out web interface. At the top, it shows the HP logo and 'iLO INTEGRATED LIGHTS-OUT'. The server name is 'Administration', the iLO name is 'ILOBJ19JTN8069E', and the user is logged in as 'Administrator'. The navigation tabs include 'System Status', 'Remote Console', 'Virtual Devices', 'Administration', and 'BL p-Class'. The left sidebar lists various management options: 'Rack Settings', 'Rack Topology', 'Server State Mgt. Module', 'Power Mgt. Module', and 'Redundant Power Mgt. Module'. The main content area is titled 'Power Management Module' and contains two sections:

**Enclosure Information**

Name	Serial Number	FW Rev	HW Rev
Accounting	0Y1962W40E88	0.92	5

Load Balance Wire	Temp (°C)	Temp Side A (°C)	Temp Side B (°C)
Not Present	34	33	28

[Return to top](#)

**Power Component General Information**

Bay Number	Occupied	AC Input	Power	FW Rev
1	Present	Good	On	1.07
2	Empty			
3	Empty			
4	Present	Failure	Off	
5	Empty			
6	Present	Failure	Off	

## Redundant Power Management Module

If the rack topology consists of a redundant power supply, the **Redundant Power Management Module** screen will be available. The **Redundant Power Management Module** screen provides the same information concerning the redundant power management module as the **Power Management Module** screen provides for the power management module.

## iLO Control of ProLiant BL p-Class Server LEDs

iLO can monitor BL p-Class servers through POST tracking and the Server Health LED.



## Server POST Tracking

There is limited feedback while the server is booting because of the headless nature of the ProLiant BL p-Class servers. iLO provides boot-time feedback by blinking the Server Health LED green during server POST. The LED is set to solid amber if the boot is unsuccessful. The LED is set to solid green at the end of a successful boot.

After a successful boot, control of the Server Health LED is returned to the server, which may turn the LED off or set it to some other color to represent the health of the server hardware.

## Insufficient Power Notification

The iLO turns the Server Health LED solid red if iLO cannot power on the server because there is insufficient power in the rack infrastructure.

## Telnet Support

Telnet access to iLO is now supported. Telnet allows text based access to the Remote Console. To use telnet the iLO Remote Console Port Configuration and Remote Console Data Encryption on the **Global Settings** screen must be configured as follows:

1. Remote Console Port Configuration must be set to **Enabled**.
2. Remote Console Data Encryption must be set to **No**.

To access iLO using Telnet:

**NOTE:** You can only open either a Telnet session or a Remote Console Session at a time, not both simultaneously. An error message will generate if both sessions are attempted at the same time.

1. Open a Telnet window.
2. When prompted, enter the IP Address or DNS Name, Login Name, and password.

**NOTE:** Access through telnet will be disabled, if the remote console port configuration on the **Global Settings** tab is set to **Disabled** or **Automatic**, or if remote console data encryption is enabled.

To terminate a Telnet session:

1. Press the **Ctrl+]** keys and the **Enter** key at the prompt.
2. If you see an extra carriage return each time the **Enter** key is pressed, press the **Ctrl+]** keys and enter `set crlf off` at the prompt.

---

# Insight Manager 7 Integration

## In This Section

Functional Overview .....	85
Identification and Association .....	85
Alerts .....	87
Port Matching .....	87
Configuring Identification of iLO .....	88
Integrating iLO with Insight Manager 7 .....	89

## Functional Overview

Insight Manager 7 enables you to:

- Identify iLO processors.
- Create an association between iLO and its server.
- Create links between iLO and its server.
- View iLO and server information and status.
- Control the amount of detailed information displayed for iLO.
- Draw a visualization of the ProLiant BL p-Class rack infrastructure.

The following sections give a summary of each function. For detailed information on these benefits and how to use Insight Manager 7, refer to the *HP Insight Manager 7 Technical Reference Guide*, provided with Insight Manager 7.

## Identification and Association

Insight Manager 7 can identify an iLO processor and create an association between iLO and server. The administrator of the iLO device may configure iLO to respond to Insight Manager 7 identification requests.

## Status

In Insight Manager 7, iLO is identified as a management processor. Insight Manager 7 displays the management processor status within the device list.

The iLO management processor is displayed as an icon in the device list on the same row as its host server. The color of the icon represents the status of the management processor.

Actions ▾ View ▾						
HW Status	Mgmt Proc	SW Status	Device Name	Device Type	Device Addresses	Product Name
			R1003	Server	170.125.1.203	ProLiant DL380
			R1004	Server	170.125.1.204	ProLiant DL380
			R1005	Server	170.125.1.205	ProLiant DL380
			R1006	Server	170.125.1.206	ProLiant DL380
			r1016	Server	170.125.1.216	ProLiant DL380
			iLO-r1016 in r1016	Management Processor	170.125.1.217	Integrated Lights-Out
			r1019	Server	170.125.1.222	ProLiant DL380
			r1021	Server	170.125.1.226	ProLiant DL380
			iLO-r1021 in r1021	Management Processor	170.125.1.227	Integrated Lights-Out
			R1022	Server	170.125.1.228	ProLiant DL380
			not 23456789	Management Processor	170.125.1.229	ProLiant DL380
			r1023	Server	170.125.1.230	ProLiant DL380
			iLO-r1023 in r1023	Management Processor	170.125.1.231	Integrated Lights-Out
			r1024	Server	170.125.1.232	ProLiant DL380
			iLO-r1024 in r1024	Management Processor	170.125.1.233	Integrated Lights-Out
			r1025	Server	170.125.1.234	ProLiant DL380
			iLO-r1025 in r1025	Management Processor	170.125.1.235	Integrated Lights-Out
			r1026	Server	170.125.1.236	ProLiant DL380
			iLO-r1026 in r1026	Management Processor	170.125.1.237	Integrated Lights-Out

Devices in table: 14 Critical 32 Major 30 Minor 108 Normal 77 Unknown - Total: 261

For a complete list of device statuses, refer to the *HP Insight Manager 7 Technical Reference Guide*, provided with Insight Manager 7.

## Queries

iLO management processors can be queried within Insight Manager 7. The administrator can save and use these queries to create groups of management processors. Refer to the *HP Insight Manager 7 Technical Reference Guide* for further details.

## Links

For ease of management, Insight Manager 7 creates links to the following locations:

- iLO and the host server from the Insight Manager 7 Home page
- iLO from the Query Results page
- The server from the Query Results page
- The server from the Device Summary page of iLO
- iLO from the Device Summary page of the server

The Home page and Query Results pages display iLO, the server, and the relationship between iLO and server. For example, the page can display the server, the iLO name next to the server, and *iLO name* **IN** *server* in the **Device Name** field for iLO.

Clicking on the device status icon for either iLO or the server takes you to the summary page of the device. Within the summary page are the status, IP address, and link for the associated device.

## Alerts

The iLO management processor can be configured to send SNMP alerts to the Insight Manager 7 console. Enter the TCP/IP address of the Insight Manager 7 console in the Management Integration page of the iLO Administration tab to direct SNMP alerts to the console.

iLO can be configured to forward alerts from the host operating system management agents, and it can also be configured to send iLO-generated alerts to the Insight Manager 7 console.

## Port Matching

Insight Manager 7 is configured to start an HTTP session to check for iLO at port 80. The port can be changed. If you want to change the port number, you must also change it in Network Settings and Insight Manager 7.

To change the port number in Insight Manager 7, add the port to the \ADDITIONALWSDISC.PROPS file. Port 80 does not need an entry in this props file, but any other port designated for iLO needs to be specified so that Insight Manager 7 can use it during HTTP identification. The format of the entries is:

```
Port=Description,Reserved 1,Reserved 2,Reserved 3,Class  
Name
```

where:

- *Port* is the number of the additional HTTP port to be added into discovery.
- *Description* is the description of the Web server to be displayed in the list of links on the device page.
- *Reserved 1* is reserved and should be set to a space.
- *Reserved 2* is reserved and should be set to true.
- *Reserved 3* is reserved and should be set to false.
- *Class Name* specifies the name of the Insight Manager 7 Java class that does the processing for the additional management processor port. This information should not be changed.

Example:

```
80=iLO, ,true,false,compaq.ID.MgmtProc.MgmtProcessorPar  
ser
```

## Configuring Identification of iLO

iLO enables you to set how much data is returned on an Insight Manager 7 request for more information.

The level of data returned is controlled on the **SNMP/Insight Manager Settings** screen. The identification data level options are:

- **High**—Associations are present and all data is present on the summary page.
- **Medium**—Associations are present but the summary page contains less detail than at high security.

- **Low**—Associations are present if SNMP pass-through is supported. If not, the server and management processor are separate entities in the device list.
- **None**—No data is returned to Insight Manager 7.

Display Information	Low	Medium	High	None
Product Name	Y	Y	Y	
Server Serial Number		Y	Y	
Server State			Y	
Management Processor Status	Y	Y	Y	
Management Processor Serial Number		Y	Y	
iLO Advanced Pack License Status and Data		Y	Y	
Hardware Revision Information			Y	
Firmware Revision Information			Y	
Rack Topology		Y	Y	
Single Sign On*			Y	
Secure Task Execution*			Y	
CIMOM*			Y	
Device Home Page URL			Y	
*Reserved for future Insight Manager 7 integration.				

## Integrating iLO with Insight Manager 7

iLO fully integrates with Insight Manager 7 in key operating environments, providing access to Insight Management agents and support for full in-band SNMP management. iLO supports SNMP trap delivery to an Insight Manager Console, which can be configured to forward SNMP traps to a pager or email.

Full integration with Insight Manager 7 also provides a single management console for launching a standard Web browser to access iLO and for providing diagnostic information about the operation of iLO. While the operating system is running, you can establish a connection to iLO using Insight Manager 7.

## Receiving SNMP Alerts in Insight Manager 7

Insight Manager 7 provides support for full SNMP management, and iLO supports SNMP trap delivery to an Insight Manager 7 console. You can view the event log, select the event, and view the additional information about the alert.

Configuring receipt of SNMP alerts in Insight Manager 7 is a two-step process. The process requires configuring Insight Manager 7 to receive SNMP alerts from an iLO-managed device and configuring iLO to enable SNMP alerts.

To configure receipt of SNMP alerts in Insight Manager 7:

1. Use the **SNMP/Insight Manager Settings** option in the **Administration** tab of the iLO navigation frame to enable SNMP alerting and to provide an SNMP trap IP address to iLO. This IP address should be the address of the computer running Insight Manager 7. Refer to the “Enabling SNMP Alerts” section for details.
2. Configure iLO as a managed device for Insight Manager 7. Adding iLO to Insight Manager 7 allows the NIC interface on iLO to function as a dedicated management port, isolating management traffic from the remote host server NIC interface.
  - a. Start Insight Manager 7. Click **Settings**. By default, the **Automatic Discovery** screen is displayed. Use this screen to discover any iLO that will be managed by Insight Manager 7. If the IP address does not already appear in the **Ping Inclusion Ranges** section, enter the IP address.
  - b. Click **Execute Discovery Now** to add iLO to Insight Manager 7. The Status section displays the system being updated.
  - c. After the discovery is complete, subsequent queries will display the device as a management processor.
  - d. You may need to select **Edit Device** from the **Discovery** tab and edit the monitor community string (for example, by changing it to “public”) so that iLO is displayed in the list of monitored devices.
  - e. iLO traps are displayed in a query for major, uncleared events. You can use the orange button at the top of the screen to issue this query. Click the event description to obtain further information about the event.



**NOTE:** HP Insight Agents for Integrated Lights-Out must be installed on the remote host server to enable management of Integrated Lights-Out by iLO. Refer to the iLO documentation for additional details about installing and configuring agents.

## Reviewing iLO Advanced Pack License Information in Insight Manager 7

Insight Manager 7 provides a report showing the license status of the iLO management processors. You may use this report to determine how many and which iLO devices are licensed for the iLO Advanced Pack.


To view this report:

1. Click **Devices**.
2. Click **Reports**.
3. Click **Device License Information—All Servers**.

The license information of the management processors is displayed. To be sure that this data is current, run the device identification task for your management processors. Refer to the Insight Manager 7 documentation for additional details about initiating tasks.


## ProLiant BL p-Class Rack Visualization

Insight Manager 7 can draw a visualization of the ProLiant BL p-Class rack, enclosures, and servers using information from iLO. The SNMP/Insight Manager setting for the level of data to be returned must be Medium or High for Insight Manager 7 to draw the visualization.

**Device: 170.10.2.4**

The following information is known about this device:  
( [Last Update](#): Tuesday January 22, 2002 - 7:45:13 AM )


**Device Information**

Status:  Normal


Address: 170.10.2.4  
Management Protocols: SNMP

Device Name: 170.10.2.4  
SNMP Alias: Au24

Contact: JP  
Location: MIMIC1  
Device Type: Server  
Product Name: ProLiant BL20p  
Description: Hardware: x86 Family 6 Model 11 Stepping 0 AT/AT COMPATIBLE - Software: Windows 2000 Version 5.0 (Build 2195 Uniprocessor Free)  
Server Role: A Very Special Server

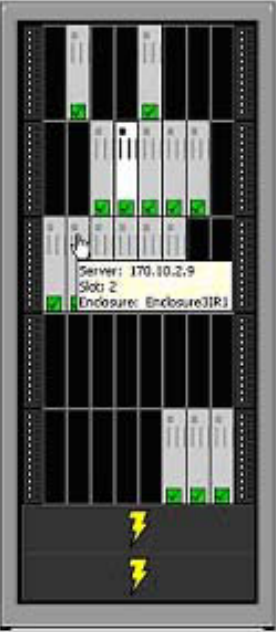
[Data Collection Report](#)  
 [SNMP Communications Settings](#)  
[All Events For This Device](#)

**Device Links**






 Normal [Compass Subsystem Status Information \(using SNMP\)](#)  
[Legacy Version Control](#)  
[SNMP Explorer](#)

**Container Information**

Rack Name: [ICFRack1](#)  
Enclosure Name: [Enclosure2R1](#)  
Slot Number: 4  
Server Dimensions: 44mm x 267mm x 711mm



**LEGEND:**

-  Server
-  Current server
-  No server identified
-  Switch
-  Power supply enclosure

---

# Security for Integrated Lights-Out

## In This Section

General Security Guidelines .....	93
Encryption .....	93
iLO Security Override Switch Administration .....	93
User Accounts .....	95
Passwords .....	96
Certificates.....	97

## General Security Guidelines

The following are general guidelines concerning security for iLO:

- For maximum security, iLO should be set up on a separate management network.
- Integrated Lights-Out should not be directly connected to the Internet.
- A 128-bit cipher strength browser must be used.

## Encryption

By default, all iLO Web pages are encrypted with Secure Sockets Layer (SSL). For security purposes, passwords are not sent across the network in a clear-text format. Passwords are not listed in clear text for the purposes of automating a login sequence. The Remote Console data is encrypted with a 128 bit RC4 bi-directional cipher.

## iLO Security Override Switch Administration

The iLO Security Override Switch allows the administrator full access to the iLO processor. This access may be necessary for any of the following conditions:

- iLO needs to be re-enabled after it has been disabled.

- All user accounts with the Administer User Accounts privilege have been locked out.
- A bad configuration keeps iLO from displaying on the network and RBSU has been disabled.
- The boot block needs to be flashed.

Ramifications of setting the Security Override Switch include:

- All security authorization checks are disabled while the switch is set.
- The iLO RBSU runs if the host server is reset.
- iLO is not disabled and may display on the network as configured.
- iLO, if disabled while the Security Override Switch is set, does not log the user out and complete the disable process until the power is cycled on the server.
- The iLO Option ROMPaq is allowed to reprogram the iLO ROM even if the iLO firmware is not running.
- The boot block is exposed for programming.

A warning message is displayed on the iLO Web pages indicating that the iLO Security Override Switch is currently in use. An iLO log entry is added recording the use of the iLO Security Override Switch. An SNMP alert may also be sent upon setting or clearing the iLO Security Override Switch.

Setting the iLO Security Override Switch also enables you to flash the iLO boot block. HP does not anticipate that you will need to update the iLO boot block. If an iLO boot block update is ever required, physical presence at the server will be required to reprogram the boot block and reset iLO. The boot block will be exposed until iLO is reset. For maximum security, HP recommends that you disconnect iLO from the network until the reset is complete.

The iLO Security Override Switch is located inside the server and cannot be accessed without opening the server enclosure. To set the iLO Security Override Switch, you need to power off the server. Set the switch and then power on the server. Reverse the procedure to clear the iLO Security Override Switch.

Depending on the server, the iLO Security Override Switch may be a single jumper or a specific switch position on a dip switch panel. To access and locate the iLO Security Override Switch, refer to the server documentation. iLO Security Override Switch can also be located using the diagrams on server hood.

## User Accounts

iLO supports the configuration of up to 12 local user accounts. Each of these accounts can be managed through the use of the following features:

- Privileges
- Global Security Settings
- Login Security

## Privileges

iLO allows the administrator to control user account access to iLO functions through the use of privileges. When a user attempts to use a function, the iLO system verifies that the user has the privilege before the user is allowed to perform the function.

Each feature available through iLO can be controlled through privileges, including Administer User Accounts, Remote Console Access, Virtual Power and Reset, Virtual Media, and Configure iLO Settings. Privileges for each user can be configured on the **User Administration** page of the **Administration** tab.

## Global Security Settings

Global security settings allow you to control access to functions or to control specific actions of functions that have been enabled globally. For example, you can control access to the iLO RBSU, enable or disable Lights-out Functionality, set the Remote Console timeout, Web server SSL and non-SSL ports, virtual media port and set the minimum password length.

## Login Security

iLO provides several login security features. After an initial failed login attempt, iLO imposes a delay of five seconds. After a second failed attempt, iLO imposes a delay of 10 seconds. After the third failed attempt, and any subsequent attempts, iLO imposes a delay of 60 seconds. All subsequent failed login attempts cycles through these values. An information page is displayed during each delay. This scenario continues until a valid login is completed. This feature assists in defending against possible dictionary attacks against the browser login port.

iLO also saves a detailed log entry for failed login attempts which imposes a delay of 60 seconds.

## Passwords

The following is a list of recommended password guidelines:

- Passwords should never be written down or recorded.
- Passwords should never be shared with others.
- Passwords should not be words generally found in a dictionary, or easy to guess words, such as the company name, product names, the user's name, or the user's User ID.
- Passwords should include at least three of the four following characteristics:
  - At least one numeric character
  - At least one special character
  - At least one lowercase character
  - At least one uppercase character

Passwords issued for a temporary User ID, password reset, or a locked out User ID should also conform to these standards. Each password must be a minimum length of zero characters and a maximum length of 39 characters. The default minimum length is set to eight characters. Setting the minimum password length to fewer than eight characters is not recommended unless you have a physically secure management network that does not extend outside the secure data center.

## Certificates

By default, iLO creates a "self-signed" certificate for use in SSL connections. This certificate enables iLO to work without any additional configuration steps. The security features of iLO can be enhanced by importing a trusted certificate.

### Importing a Certificate

- **Create Certificate Request**—iLO can create a CR (in PKCS #10 format) which can be sent to a CA. This certificate request is base64 encoded. A CA will process this request and return a response (X.509 Certificate) which can be imported into Integrated Lights-Out. Everytime the **Create Certificate Request** button is clicked, a new certificate request is generated even though the iLO name is same.

The CR contains a public/private key pair that will be used for validation of communications between the client browser and iLO. The generated CR is held in memory until a new CR is generated; a certificate is imported via this process; or iLO is reset. This means you can generate the CR and copy it to the client clipboard, leave the iLO web site to retrieve the certificate, then return to import the certificate.

When submitting the request to the CA, insure you

- use the iLO name as listed on the **System Status** screen as the URL for the server;
  - request the certificate be generated in the RAW format;
  - include the `Begin` and `End` certificate lines.
- **Import Certificate**—If you are returning to this page with a certificate to import, clicking the **Import Certificate** button enables you to go directly to the **Certificate Import** screen without generating a new CR. This is important in that a given certificate will only work with the keys contained in the CR from which the certificate was generated. If iLO has been reset or another CR has been generated since the CR that was used to request the certificate was generated, then another CR will must be generated and a new certificate procured from the CA.

# Directory Services

## In This Section

Introduction to Directory Services .....	99
Schema Documentation.....	99
Directory Services Support.....	100
Required Software .....	101
Schema Installer .....	101
Management Snap-In Installer.....	104
Directory Services for Active Directory.....	105
Directory Services for eDirectory.....	122
Configuring Directory Settings .....	135
User Login to iLO.....	138

## Introduction to Directory Services

The iLO Directory Services functionality, available with firmware version 1.40 or later, enables you to:

- Authenticate users from a shared consolidated, scalable user database.
- Control user privileges (authorization) using the directory service.
- Use Roles in the directory service for group level administration of iLO management processors and iLO users.

**IMPORTANT:** Installing Directory Services for Integrated Lights-Out requires extending the directory schema. Extending the schema must be completed by a Schema Administrator.

## Schema Documentation

To assist with the planning and approval process, HP provides up-front documentation on the changes made to the schema during the schema setup process. The *HP Directory Services Schema Information Booklet* is available on the HP website (<http://www.hp.com/servers/lights-out>).



## Directory Services Support

iLO supports the following directory services:

- Microsoft® Active Directory
- Microsoft® Windows® Server 2003 Active Directory
- Novell eDirectory 8.6.2
- Novell eDirectory 8.7

The iLO software is designed to run within the Microsoft® Active Directory Users and Computers and Novell ConsoleOne management tools, allowing you to manage user accounts on Microsoft Active Directory or Novell eDirectory. This solution makes no distinction between eDirectory running on NetWare, Linux, or Windows®. To spawn an eDirectory schema extension requires Java 1.4.0 or later for SSL authentication.

iLO supports Microsoft® Active Directory running on one of the following operating systems:

- Windows® 2000
- Windows® 2000 Advanced Server
- Windows® Server 2003

iLO supports eDirectory 8.6.2 and 8.7 running on one of the following operating systems:

- Windows® 2000
- Windows® 2000 Advanced Server
- Windows® Server 2003
- NetWare 5.X
- NetWare 6.X
- Red Hat Enterprise Linux AS 2.1

- Red Hat Linux 7.3
- Red Hat Linux 8.0

## Required Software

iLO requires specific software, which will extend the schema and provide snap-ins to manage your iLO network. An HP Smart Component is available for download that contains the schema installer and the management snap-in installer. The HP Smart Component can be downloaded from the HP website (<http://www.hp.com/servers/lights-out>).

## Schema Installer

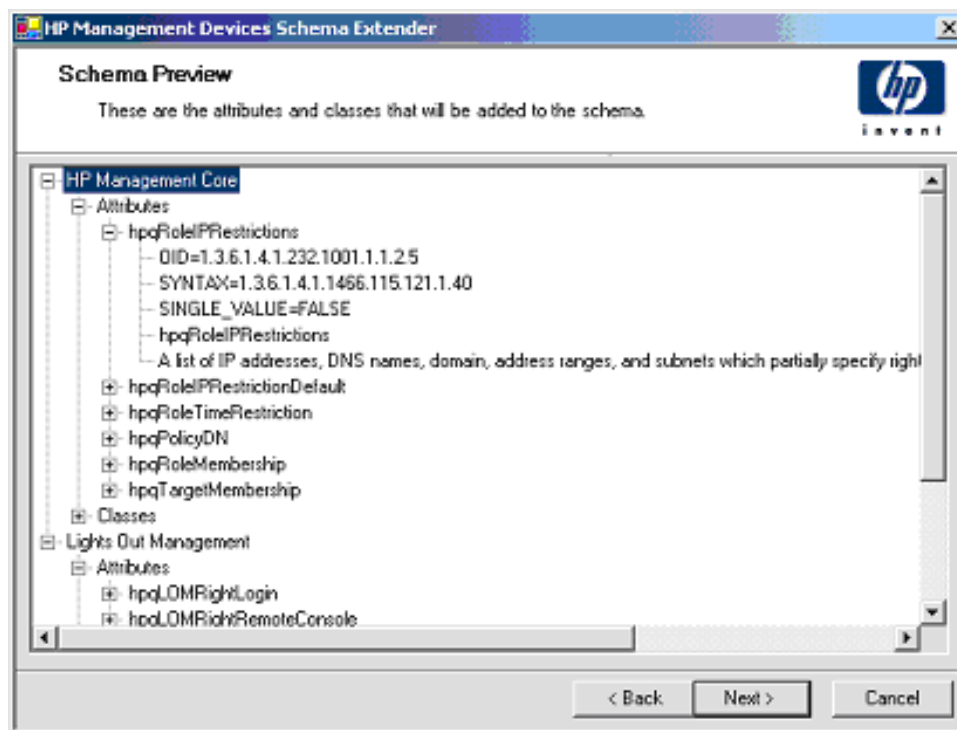
Bundled with the schema installer are one or more .xml files. These files contain the schema that will be added to the directory. Typically, one of these files will contain core schema that is common to all the supported directory services. Additional files contain only product-specific schemas. The schema installer requires the use of the .NET framework.

The installer includes three important screens:

- Schema Preview
- Setup
- Results

## Schema Preview

The **Schema Preview** screen allows the user to view the proposed extensions to the schema. This screen reads the selected schema files, parses the XML, and displays it as a tree view. It lists all of the details of the attributes and classes that will be installed.



## Setup

The **Setup** screen is used to enter the appropriate information before extending the schema.

The **Directory Server** section of the **Setup** screen enables you to select whether you will be using Active Directory or eDirectory, and to set the computer name and the port to be used for LDAP communications.

**IMPORTANT:** Extending the schema on **Active Directory** requires that the user be an authenticated Schema Administrator, that the schema is not write protected, and the directory is the FSMO role owner in the tree. The installer will attempt to make the target directory server the FSMO Schema Master of the forest.

To get write access to the schema on Windows® 2000 requires a change to the registry safety interlock. If the user selects the **Active Directory** option, the schema extender will attempt to make the registry change. It will only succeed if the user has rights to do this. Write access to the schema is automatically enabled on Windows® Server 2003.

The **Directory Login** section of the **Setup** screen enables you to enter your login name and password. These may be required to complete the schema extension. The **Use SSL during authentication** option sets the form of secure authentication to be used. If not selected, NT authentication is used for Active Directory, and clear text authentication is used for eDirectory.

HP Management Devices Schema Extender

**Setup**

The wizard needs to know about the directory you will be accessing.

**Directory Server**

☒ Active Directory ☐ eDirectory

Name: compaq-2loseval

Port: 636

**Directory Login**

Login Name: JPDOMAIN\_LAB\Administrator

Password:

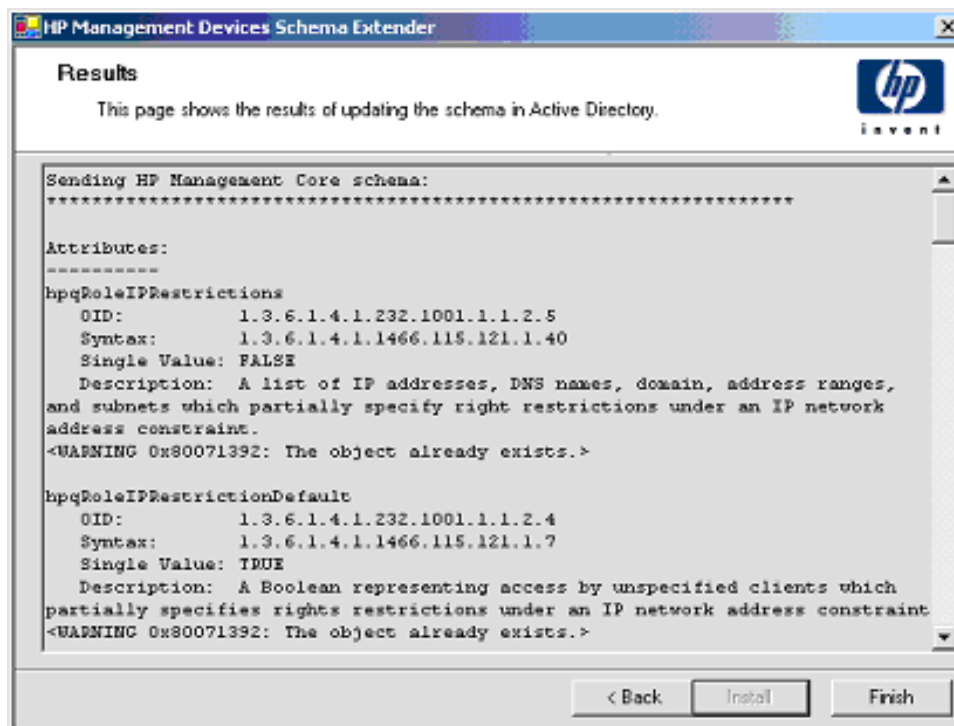
☐ Use SSL during authentication.

When you press the "Install" button, the wizard will begin extending the schema.

< Back Install Cancel

## Results

The **Results** screen displays the results of the installation, including whether the schema could be extended and what attributes were changed.



## Management Snap-In Installer

The management snap-in installer installs the snap-ins required to manage iLO objects in a Microsoft® Active Directory Users and Computers directory or Novell ConsoleOne directory.

The iLO snap-ins are used to perform the following tasks in creating an iLO directory:

- Creating and managing the iLO and role objects (policy objects will be supported at a later date).

- Making the associations between iLO objects and the role (or policy) objects.

## Directory Services for Active Directory

The following sections provide installation prerequisites, preparation, and a working example of Directory Services for Active Directory.

### Active Directory Installation Prerequisites

Directory Services for iLO uses LDAP over SSL to communicate with the directory servers. Before installing snap-ins and schema for Active Directory, read and have available the following documentation:

**IMPORTANT:** Installing Directory Services for Integrated Lights-Out requires extending the Active Directory schema. Extending the schema must be completed by an Active Directory Schema Administrator.

- *Extending the Schema* in the Microsoft® Windows® 2000 Server Resource Kit, available at <http://msdn.microsoft.com>
- *Installing Active Directory* in the Microsoft® Windows® 2000 Server Resource Kit
- Microsoft® Knowledge Base Articles
  - 216999 *Installing the remote server administration tools in Windows® 2000*
  - 314978 *Using the Adminpak.msi to install a server administration tool in Windows® 2000*
  - 247078 *Enabling SSL communication over LDAP for Windows® 2000 domain controllers*
  - 321051 *Enabling LDAP over SSL with a third-party certificate authority*
  - 299687 *MS01-036: Function Exposed By Using LDAP over SSL Could Enable Passwords to Be Changed*

### Directory Services Preparation for Active Directory

To set up directory services for use with iLO management processors:

1. Install Active Directory. For more information, refer to *Installing Active Directory* in the Microsoft® Windows® 2000 Server Resource Kit.
2. Install the Microsoft® Admin Pack (the ADMINPAK.MSI file, which is located in the i386 subdirectory of the Windows® 2000 Server or Advance Server CD). For more information, refer to the Microsoft® Knowledge Base Article 216999.
3. In Windows® 2000, the safety interlock that prevents accidental writes to the schema needs to be temporarily disabled. The schema extender utility will be able to do this if the remote registry service is running and the user has sufficient rights. This can also be done by setting *HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\Parameters\Schema Update Allowed* in the registry to a non-zero value (refer to the "Order of Processing When Extending the Schema" section of *Installation of Schema Extensions* in the Windows® 2000 Server Resource Kit) or by the following steps.

**IMPORTANT:** Incorrectly editing the registry can severely damage your system. HP recommends creating a back up of any valued data on the computer before making changes to the registry.

**NOTE:** This step is not necessary if you are using Windows® Server 2003.

- a. Start MMC.
  - b. Install the Active Directory Schema snap-in in MMC.
  - c. Right-click **Active Directory Schema** and select **Operations Master**.
  - d. Select **The Schema may be modified on this Domain Controller**.
  - e. Click **OK**.
- NOTE:** The **Active Directory Schema** folder may need to be expanded for the check box to be available.
4. Create a certificate or install Certificate Services. This step is necessary to create a certificate or install Certificate Services because iLO communicates with Active Directory using SSL. Active Directory must be installed before installing Certificate Services.
  5. To specify that a certificate be issued to the server running active directory, do the following:

- a. Launch Microsoft Management Console on the server and add the default domain policy snap-in (Group Policy, then browse to Default domain policy object).
  - b. Click **Computer Configuration, Windows Settings, Security Settings, Public Key Policies**.
  - c. Right-click **Automatic Certificate Requests Settings**, and select **new, automatic certificate request**.
  - d. Using the wizard, select the domain controller template, and the certificate authority you want to use.
6. Download the Smart Component, which contains the installers for the schema extender and the snap-ins. The Smart Component can be downloaded from the HP website (<http://www.hp.com/servers/lights-out>).
  7. Run the schema installer application to extend the schema, which extends the directory schema with the proper HP objects.

**NOTE:** The schema installer associates the Active Directory snap-ins with the new schema. The snap-in installation setup utility is a Windows MSI setup script and will run anywhere MSI is supported (Windows® XP, Windows® 2000, Windows® 98). However, some parts of the schema extension application require the .NET Framework, which can be downloaded from [www.microsoft.com](http://www.microsoft.com).

## Snap-in Installation and Initialization for Active Directory

1. Run the snap-in installation application to install the snap-ins.
2. Configure the directory service to have the appropriate objects and relationships for iLO management.
  - a. Use the management snap-ins from HP to create iLO, Policy, Admin, and User Role objects.
  - b. Use the management snap-ins from HP to build associations between the iLO object, the policy object, and the role object.
  - c. Point the iLO object to the Admin and User role objects (Admin and User roles will automatically point back to the iLO object).

**NOTE:** For more information on Integrated Lights-Out objects, see "Directory Services Objects".

At a minimum, you must create:

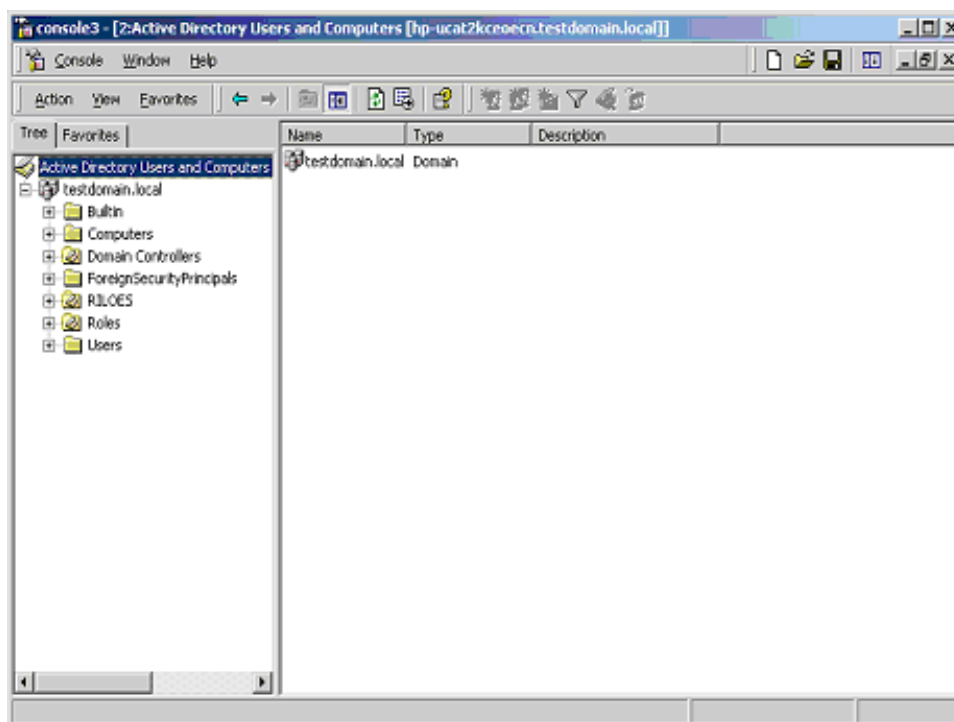


- One Role object that will contain one or more users and one or more iLO objects.
- One iLO object corresponding to each iLO management processor that will be using the directory.

### Example: Creating and Configuring Directory Objects for Use with iLO in Active Directory

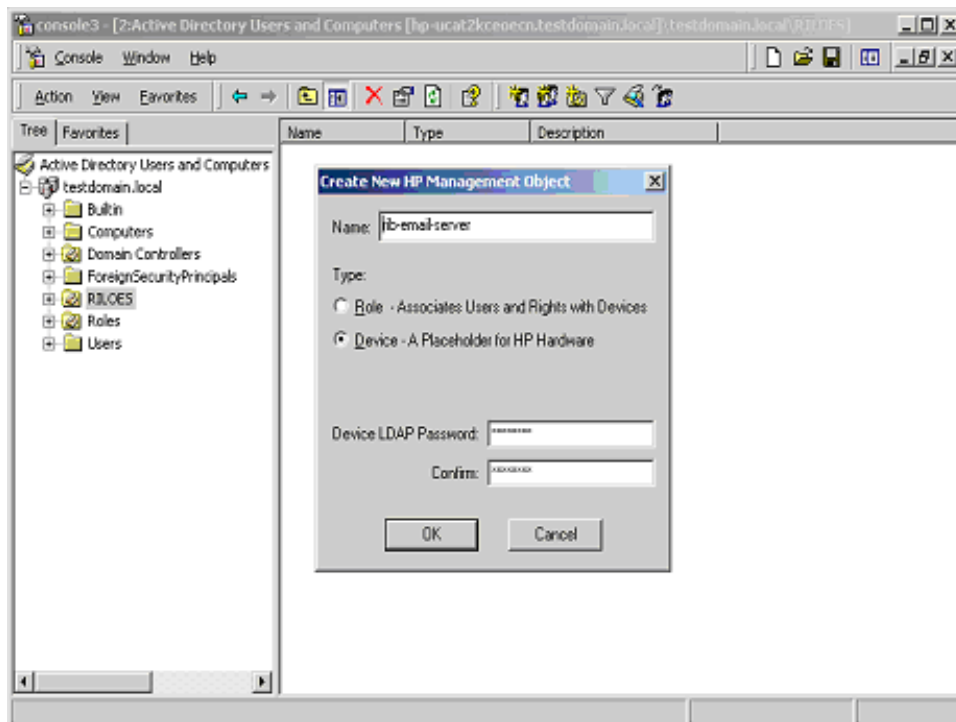
The following example shows how to set up roles and HP devices in an enterprise directory with the domain *testdomain.local*, which consists of two organizational units, *Roles* and *RILOES*.

Assume that a company has an enterprise directory including the domain *testdomain.local* arranged as shown in the following screen.



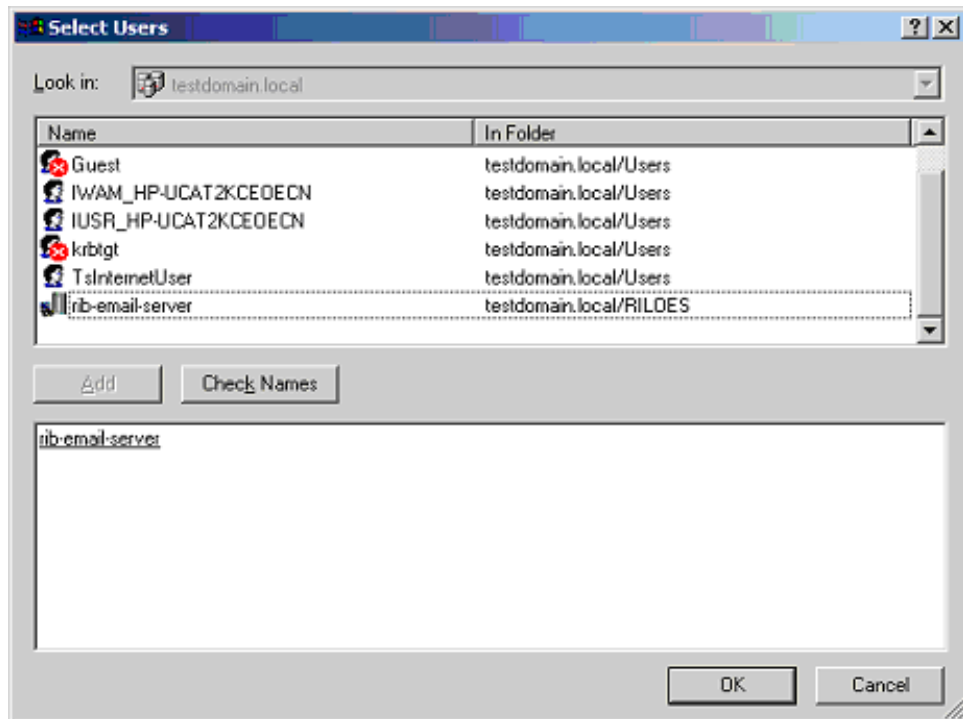
1. Create an organizational unit, which will contain the Lights-Out Devices managed by the domain. In this example, two organizational units are created called *Roles* and *RILOES*.
2. Use the HP provided Active Directory Users and Computers snap-ins to create Lights-Out Management objects in the *RILOES* organizational unit for several iLO devices.
  - a. Right-click the **RILOES** organizational unit found in the *testdomain.local* domain, and select **NewHPObject**.
  - b. Select **Device** for the type on the **Create New HP Management Object** dialog box.
  - c. Enter an appropriate name in the **Name** field of the dialog box. In this example, the DNS host name of the iLO device, *rib-email-server*, will be used as the name of the Lights-Out Management object, and the surname will be *RILOEII*.
  - d. Enter and confirm a password in the **Device LDAP Password** and **Confirm** fields. The device will use this password to authenticate to the directory, and should be unique to the device. This password is the password that is used in the **Directory Settings** screen of the iLO.

- e. Click **OK**.

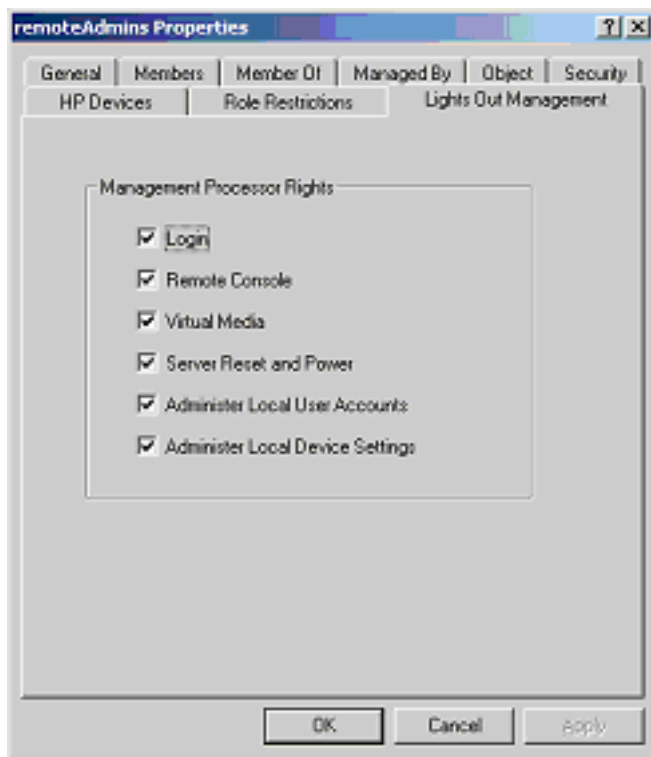


3. Use the HP provided Active Directory Users and Computers snap-ins to create HP Role objects in the *Roles* organizational unit.
  - a. Right-click the **Roles** organizational unit, select **New** then **Object**.
  - b. Select **Role** for the type field in the **Create New HP Management Object** dialog box.
  - c. Enter an appropriate name in the **Name field** of the **New HP Management Object** dialog box. In this example, the role will contain users trusted for remote server administration and will be called *remoteAdmins*. Click **OK**.
  - d. Repeat the process, creating a role for remote server monitors called *remoteMonitors*.
4. Use the HP provided Active Directory Users and Computers snap-ins to assign the roles rights, and associate the roles with users and devices.

- a. Right-click the **remoteAdmins** role in the Roles organizational unit in the *testdomain.local* domain, and select **Properties**.
- b. Select the **HP Devices** tab, then click **Add**.
- c. Using the **Select Users** dialog box, select the Lights-Out Management object created in step 2, *rib-email-server* in folder *testdomain.local/RILOES*. Click **OK** to close the dialog, then click **Apply** to save the list.



- d. Add users to the role. Click the **Members** tab, and add users using the **Add** button and the **Select Users** dialog box.



5. The devices and users are now associated. Use the **Lights Out Management** tab to set the rights for the role. All users and groups within a role will have the rights assigned to the role on all of the iLO devices managed by the role. In this example, the users in the *remoteAdmins* role will be given full access to the iLO functionality. Select the boxes next to each right, and then click **Apply**. Click **OK** to close the property sheet.
6. Using the same procedure as in step 4, edit the properties of the *remoteMonitors* role, add the *rib-email-server* device to the **Managed Devices** list on the **HP Devices** tab, and add users to the *remoteMonitors* role using the **Members** tab. Then, on the **Lights Out Management** tab, select the box next to the **Login**. Click **Apply** and **OK**. Members of the *remoteMonitors* role will be able to authenticate and view the server status.

User rights to any Integrated Lights-Out device are calculated as the sum of all the rights assigned by all the roles in which the user is a member, and in which the Integrated Lights-Out device is a Managed Device. Following the preceding examples, if a user is in both the *remoteAdmins* and *remoteMonitors* roles, they will have all the rights, because the *remoteAdmins* role has those rights.

To configure a Integrated Lights-Out device and associate it with a Lights-Out Management object used in this example, use settings similar to the following on the **Directory Settings** screen.

```
RIB Object DN = cn=rib-email-  
server,ou=RILOES,dc=testdomain,dc=local  
Directory User Context 1 =  
cn=Users,dc=testdomain,dc=local
```

For example, to gain access, user *Mel Moore*, with the unique ID *MooreM*, located in the users organizational unit within the *testdomain.local* domain, who is also a member of one of the *remoteAdmins* or *remoteMonitors* roles, would be allowed to log in to the iLO. They would type `testdomain\moorem`, or `moorem@testdomain.local`, or *Mel Moore*, in the **Login Name** field of the iLO login screen, and use their Active Directory password in the **Password** field of that screen.

## Directory Services Objects for Active Directory

One of the keys to directory-based management is proper virtualization of the managed devices in the directory service. This virtualization allows the administrator to build relationships between the managed device and user or groups already contained within the directory service. User management of a Integrated Lights-Out requires three basic objects in the directory service:

- Lights-Out Management object
- Role object
- User objects

Each object represents a device, user, or relationship that is required for directory-based management.

**NOTE:** After the snap-ins are installed, ConsoleOne and MMC must be restarted to show the new entries.

After the snap-in is installed, Integrated Lights-Out objects and Integrated Lights-Out roles can be created in the directory. Using the Users and Computers tool, the user will:

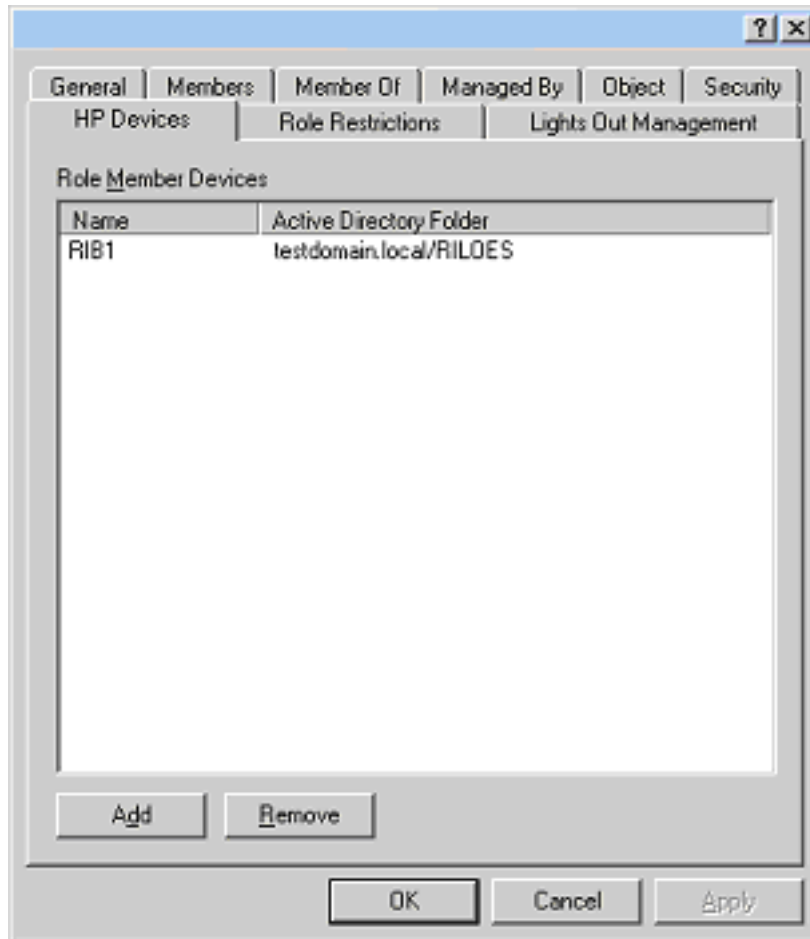
- Create the Integrated Lights-Out and role objects.
- Add users to the role objects.
- Set the rights and restrictions of the role objects.

### **Active Directory Snap-Ins**

The following sections discuss the additional management options available within Active Directory Users and Computers after the HP snap-ins have been installed.

## HP Devices

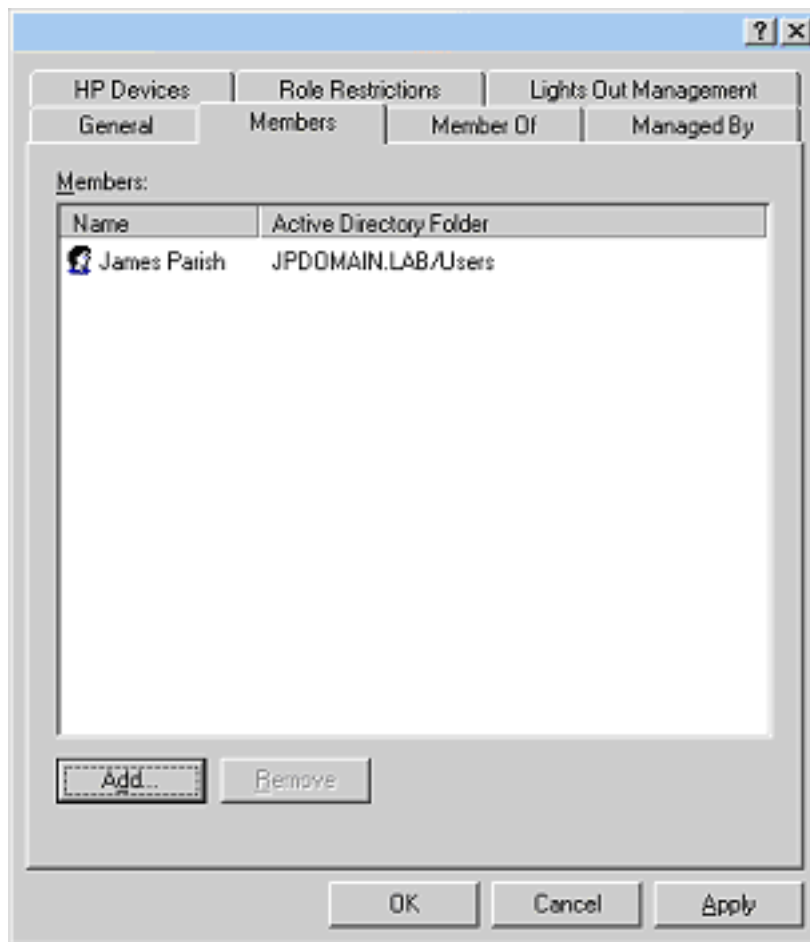
The **HP Devices** tab is used to add the HP devices to be managed within a role. Clicking **Add** enables you to browse to a specific HP device and add it to the list of member devices. Clicking **Remove** enables you to browse to a specific HP device and remove it from the list of member devices.





## Members

After user objects are created, the **Members** tab enables you to manage the users within the role. Clicking **Add** enables you to browse to the specific user you want to add. Highlighting an existing user and clicking **Remove** removes the user from the list of valid members.



## Role Restrictions

The **Role Restrictions** subtab allows you to set login restrictions for the role. These restrictions include:

- Time Restrictions
- IP Network Address Restrictions
  - IP/Mask
  - IP Range
  - DNS Name

General Members Member Of Managed By  
HP Devices Role Restrictions Lights Out Management

Time Restrictions:  
Effective Hours

IP Network Address Restrictions:  
By Default, Grant access from all clients, EXCEPT those listed below.

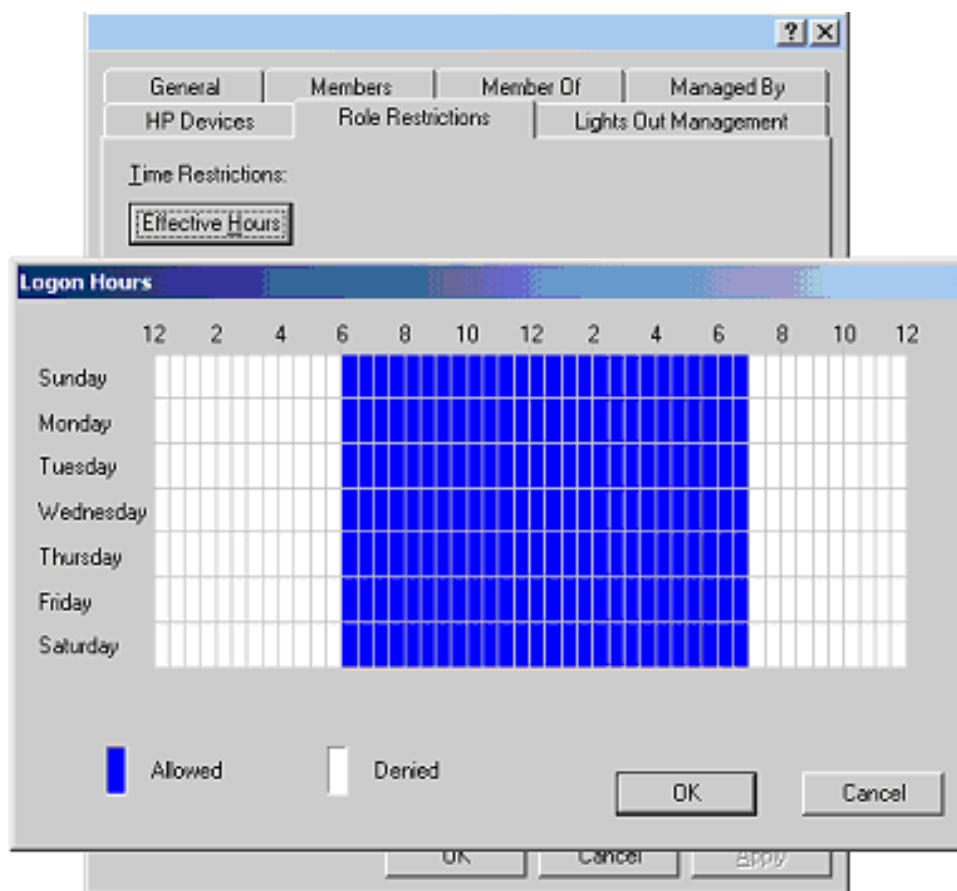
☒ IP/MASK ☐ IP Range ☐ DNS Name

Add  
Remove

OK Cancel Apply

## Time Restrictions

You can manage the hours available for logon by members of the role by clicking **Effective Hours** in the **Role Restrictions** tab. In the **Logon Hours** pop-up window, you can select the times available for logon for each day of the week in half-hour increments. You can change a single square by clicking it, or you can change a section of squares by clicking and holding the mouse button, dragging the cursor across the squares to be changed, and releasing the mouse button. The default setting is to allow access at all times.



## Enforced Client IP Address or DNS Name Access

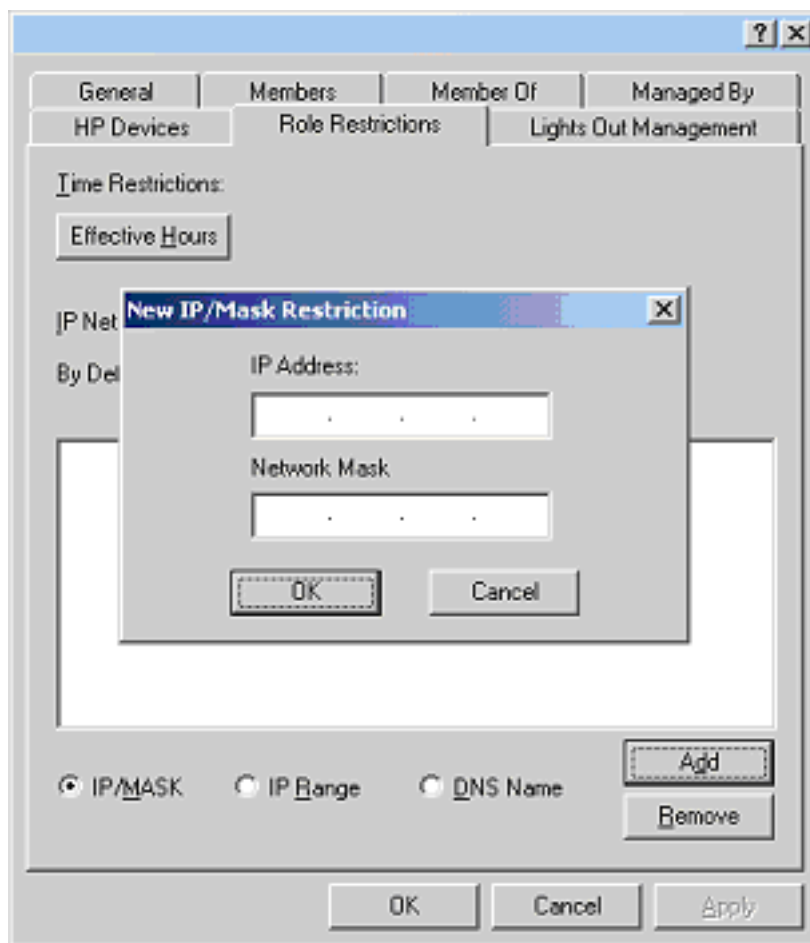
Access can be granted or denied to an IP address, IP address range, or DNS names.

1. In the **By Default** drop-down menu, select whether to **Grant** or **Deny** access from all addresses except the specified IP addresses, IP address ranges, and DNS names.
2. Select the addresses to be added, select the type of restriction, and click **Add**.
3. In the new restriction popup window, enter the information and click **OK**. The new restriction popup window displays.

**NOTE:** The **DNS Name** option allows you to restrict access based on a single DNS name or a subdomain, entered in the form of host.company.com or \*.domain.company.com.

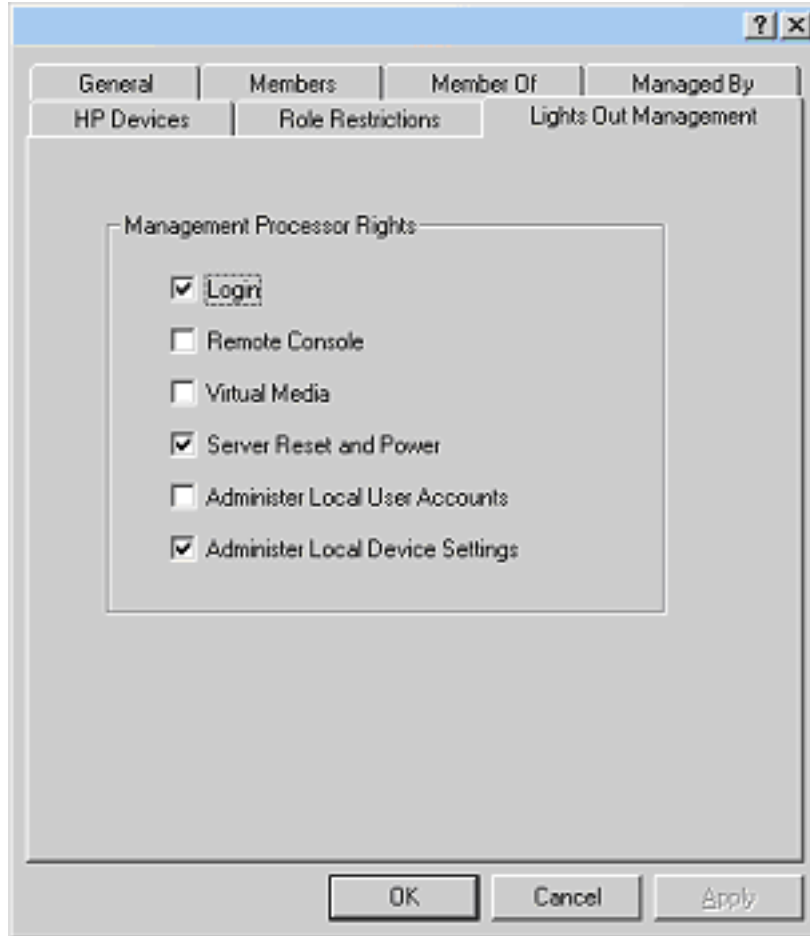
4. Click **OK** to save the changes.

5. To remove any of the entries, highlight the entry in the display list and click **Remove**.



## Active Directory Lights-Out Management

After a role is created, rights for the role can be selected. Users and group objects can now be made members of the role, giving the users or group of users the rights granted by the role. Rights are managed on the **Lights Out Management** tab.



The available rights are:

- **Login**—This option controls whether users can log in to the associated devices.

- **Remote Console**—This option enables the user access to the **Remote Console**.
- **Virtual Media**—This option enables the user access to the iLO virtual media functionality.
- **Server Reset and Power**—This option enables the user access to the iLO **Virtual Power** button to remotely reset the server or power it down.
- **Administer Local User Accounts**—This option enables the user to administer accounts. The user can modify their account settings, modify other user account settings, add users, and delete users.
- **Administer Local Device Settings**—This option enables the user to configure the iLO management processor settings. These settings include the options available on the **Global Settings**, **Network Settings**, **SNMP Settings**, and **Directory Settings** screens of the iLO Web browser.

## Directory Services for eDirectory

The following sections provide installation prerequisites, preparation, and a working example of Directory Services for eDirectory.

### eDirectory Installation Prerequisites

Directory Services for iLO uses LDAP over SSL to communicate with the directory servers. The iLO software is designed to install in an eDirectory version 8.6.1 (and above) tree. HP does not recommend installing this product if you have eDirectory servers with a version less than eDirectory 8.6.1. Before installing snap-ins and schema extensions for eDirectory, you should read and have available the following technical information documents, available at Novell Support (<http://support.novell.com>).

**IMPORTANT:** Installing Directory Services for Integrated Lights-Out requires extending the eDirectory schema. Extending the schema must be completed by a Schema Administrator.

- TID10066591 *Novell eDirectory 8.6 NDS compatibility*
- TID10057565 *Unknown objects in a mixed environment*
- TID10059954 *How to test whether LDAP is working correctly*

- TID10023209 *How to configure LDAP for SSL (secure) connections*
- TID10075010 *How to test LDAP authentication*

## Snap-in Installation and Initialization for eDirectory

1. Run the snap-in installation application to install the snap-ins.
2. Configure the directory service to have the appropriate objects and relationships for iLO management.
  - a. Use the management snap-ins from HP to create iLO, Policy, Admin, and User Role objects.
  - b. Use the management snap-ins from HP to build associations between the iLO object, the policy object, and the role object.
  - c. Point the iLO object to the Admin and User role objects (Admin and User roles will automatically point back to the iLO object).

**NOTE:** For more information on Integrated Lights-Out objects, see "Directory Services Objects".

At a minimum, you must create:

- One Role object that will contain one or more users and one or more iLO objects.
- One iLO object corresponding to each iLO management processor that will be using the directory.

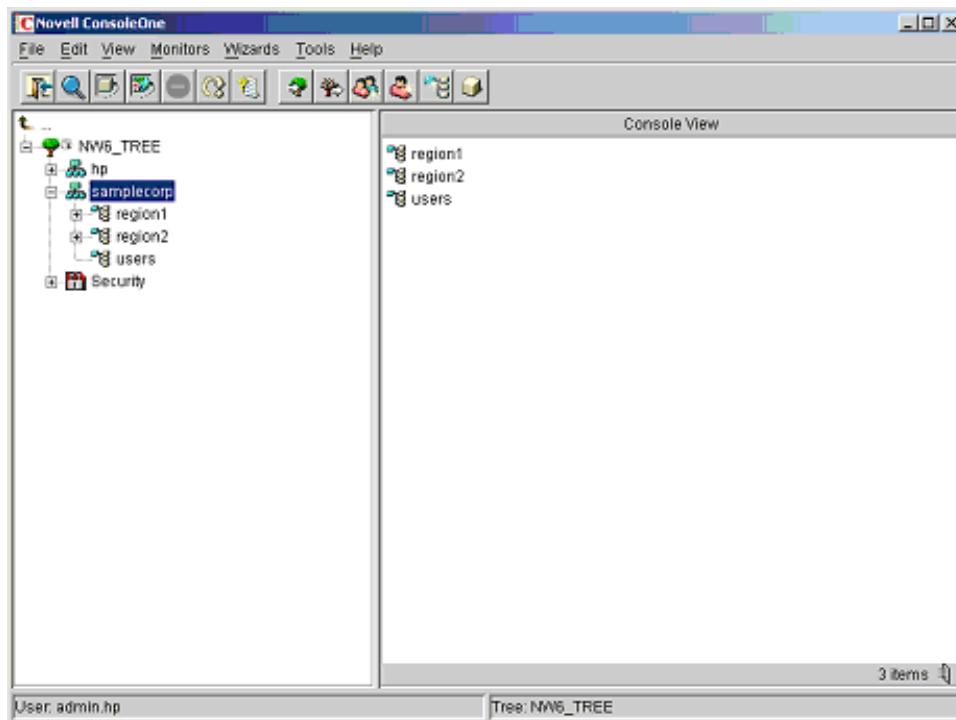
**NOTE:** After the snap-ins are installed, ConsoleOne and MMC must be restarted to show the new entries.

### Example: Creating and Configuring Directory Objects for Use with iLO in eDirectory

The following example shows how to set up roles and HP devices in a company called *samplecorp*, which consist of two regions, *region1* and *region2*.

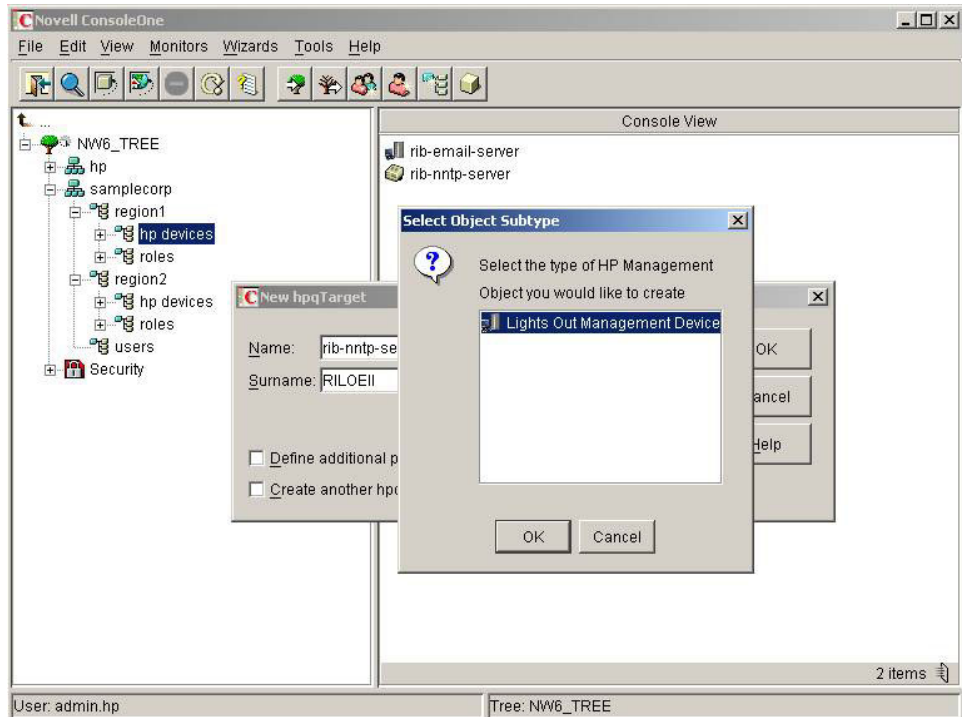


Assume *samplecorp* has an enterprise directory arranged according to the following screen.



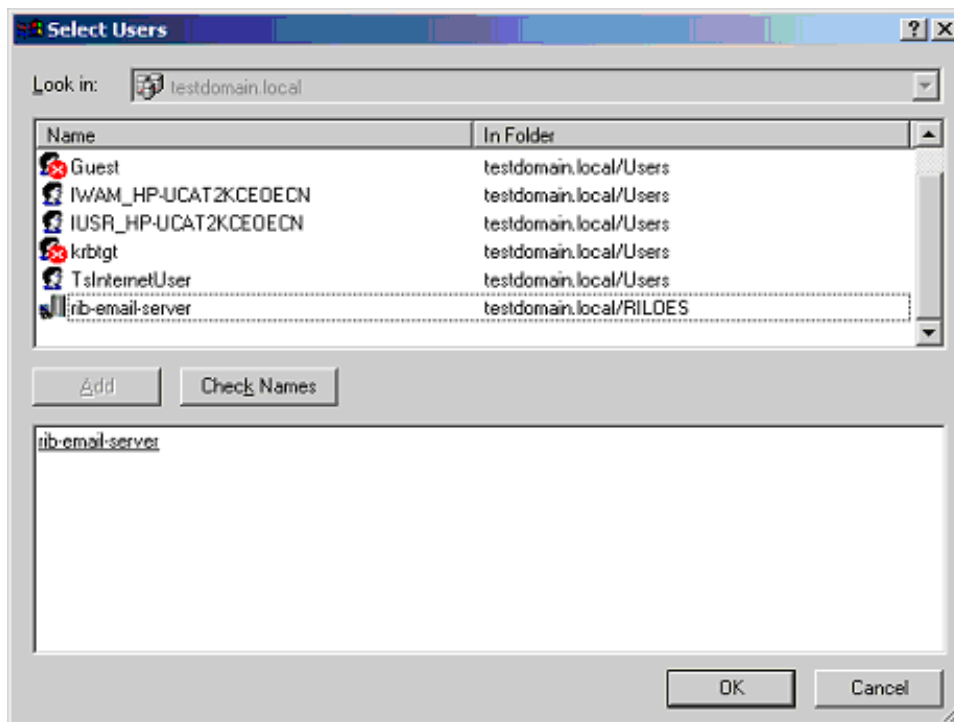
1. Begin by creating organizational units in each region, which will contain the Lights-Out Management devices and roles specific to that region. In this example, two organizational units are created, called *roles* and *hp devices*, in each organizational unit, *region1* and *region2*.
2. Use the HP provided ConsoleOne snap-ins to create Lights-Out Management objects in the *hp devices* organizational unit for several iLO devices.
  - a. Right-click the *hp devices* organizational unit found in the *region1* organizational unit, and select **New** then **Object**.
  - b. Select **hpqTarget** from the list of classes and click **OK**.
  - c. Enter an appropriate name and surname in the **New hpqTarget** dialog box. In this example, the DNS host name of the iLO device, *rib-email-server* will be used as the name of the Lights-Out Management object, and the surname will be *RILOEII*. Click **OK**.

- d. The **Select Object Subtype** dialog box is displayed. Select **Lights Out Management Device** from the list, and click **OK**.
- e. Repeat the process for several more iLO devices with DNS names *rib-nntp-server* and *rib-file-server-users1* in *hp* devices under *region1*, and *rib-file-server-users2* and *rib-app-server* in *hp* devices under *region2*.

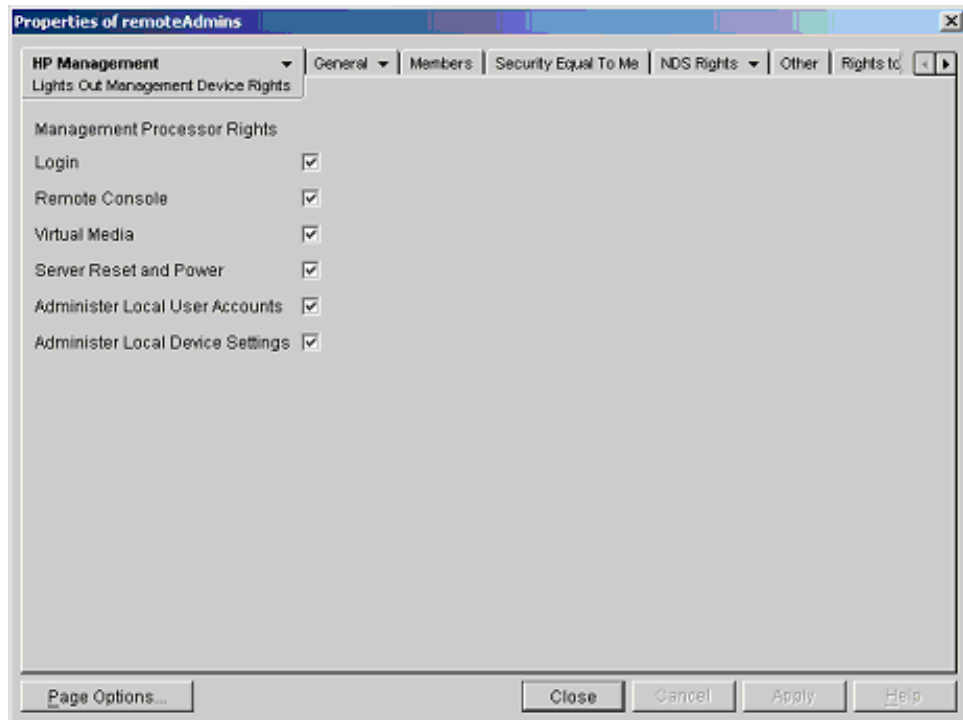


3. Use the HP provided ConsoleOne snap-ins to create HP Role objects in the *roles* organizational units.
  - a. Right-click the *roles* organizational unit found in the *region2* organizational unit, and select **New** then **Object**.
  - b. Select **hpqRole** from the list of classes and click **OK**.
  - c. Enter an appropriate name in the **New hpqRole** dialog box. In this example, the role will contain users trusted for remote server administration and will be named *remoteAdmins*. Click **OK**.

- d. The **Select Object Subtype** dialog box is displayed. Because this role will be managing the rights to Lights-Out Management devices, select **Lights Out Management Devices** from the list, and click **OK**.
      - e. Repeat the process, creating a role for remote server monitors, named *remoteMonitors*, in *roles* in *region1*, and a *remoteAdmins* and a *remoteMonitors* role in *roles* in *region2*.
  4. Use the HP provided ConsoleOne snap-ins to assign rights to the role and associate the roles with users and devices.
    - a. Right-click on the *remoteAdmins* role in the *roles* organizational unit in the *region1* organizational unit, and select **Properties**.
    - b. Select the **Role Managed Devices** subtab of the **HP Management** tab, and click **Add**.



- c. Using the **Select Objects** dialog box, browse to the *hp devices* organizational unit in the *region1* organizational unit. Select the three Lights-Out Management objects created in step 2. Click **OK**, then click **Apply**.
- d. Next, add users to the role. Click the **Members** tab, and add users using the **Add** button and the **Select Object** dialog box.
- e. The devices and users are now associated. Use the **Lights Out Management Device Rights** subtab of the **HP Management** tab to set the rights for the role. All users within a role will have the rights assigned to the role on all of the iLO devices managed by the role. In this example, the users in the *remoteAdmins* role will be given full access to the iLO functionality. Select the boxes next to each right, and click **Apply**. Click **Close** to close the property sheet.



5. Using the same procedure as in step 4, edit the properties of the *remoteMonitors* role:

- a. Add the three iLO devices within *hp devices* under *region1* to the **Managed Devices** list on the **Role Managed Devices** subtab of the **HP Management** tab.
- b. Add users to the *remoteMonitors* role using the **Members** tab.
- c. Then, using the **Lights Out Management Device Rights** subtab of the **HP Management** tab, select the check box next to **Login**, and click **Apply** and **Close**. Members of the *remoteMonitors* role will be able to authenticate and view the server status.

User rights to any Integrated Lights-Out device are calculated as the sum of all the rights assigned by all the roles in which the user is a member, and in which the Integrated Lights-Out device is a Managed Device. Following the preceding examples, if a user is in both the *remoteAdmins* and *remoteMonitors* roles, they will have all the rights, because the *remoteAdmins* role has those rights.

To configure a Integrated Lights-Out device and associate it with a Lights-Out Management object used in this example, use settings similar to the following on the **Directory Settings** screen.

**NOTE:** Commas, not periods, are used in LDAP distinguished names to separate each component.

```
RIB Object DN = cn=rib-email-server,ou=hp
devices,ou=region1,o=samplecorp
Directory User Context 1 = ou=users,o=samplecorp
```

For example, user *CSmith*, located in the *users* organizational unit within the *samplecorp* organization, who is also a member of one of the *remoteAdmins* or *remoteMonitors* roles, would be allowed to log in to the iLO. They would type *csmith* (case insensitive) in the **Login Name** field of the iLO login screen and use their eDirectory password in the **Password** field of that screen to gain access.

## Directory Services Objects for eDirectory

One of the keys to directory-based management is proper virtualization of the managed devices in the directory service. This virtualization allows the administrator to build relationships between the managed device and user or groups already contained within the directory service. User management of a Integrated Lights-Out requires three basic objects in the directory service:

- Lights-Out Management object

- Role object
- User objects

Each object represents a device, user, or relationship that is required for directory-based management.

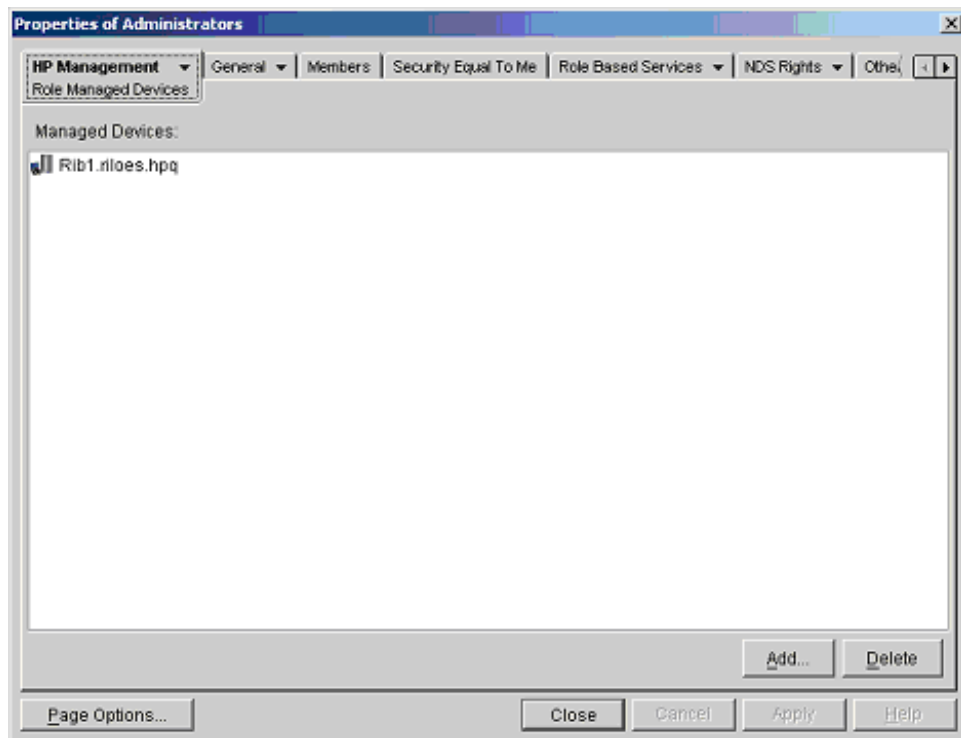
**NOTE:** After the snap-ins are installed, ConsoleOne and MMC must be restarted to show the new entries.

After the snap-in is installed, Integrated Lights-Out objects and Integrated Lights-Out roles can be created in the directory. Using the Users and Computers tool, the user will:

- Create the Integrated Lights-Out and role objects.
- Add users to the role objects.
- Set the rights and restrictions of the role objects.

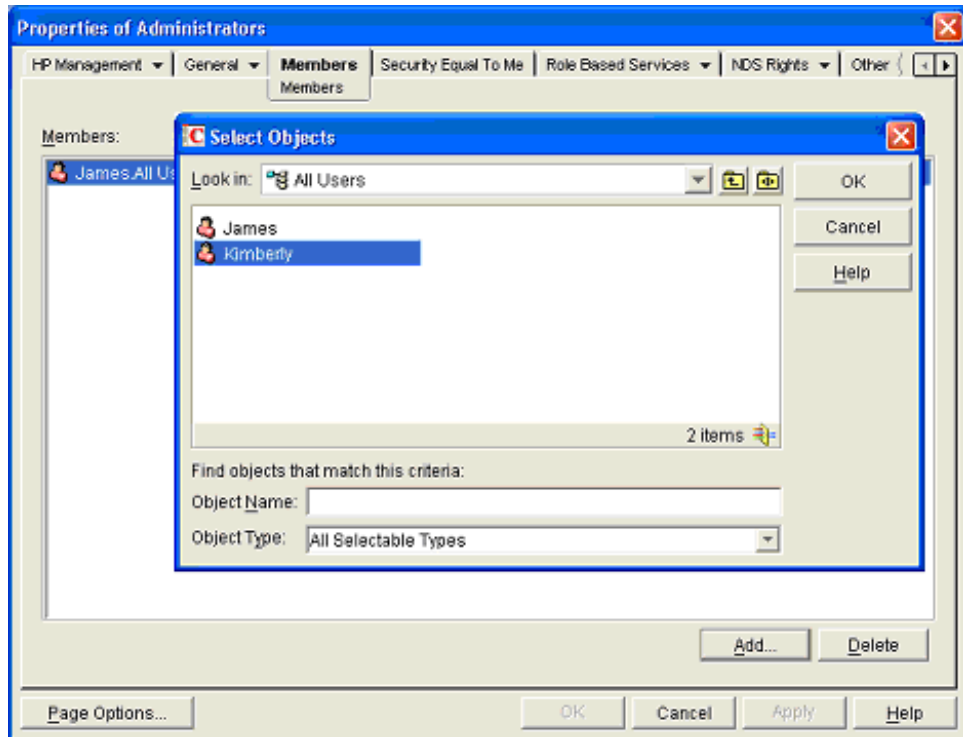
## Role Managed Devices

The **Role Managed Devices** subtab under the **HP Management** tab is used to add the HP devices to be managed within a role. Clicking **Add** allows you to browse to the specific HP device and add it as a managed device.



## Members

After user objects are created, the **Members** tab allows you to manage the users within the role. Clicking **Add** allows you to browse to the specific user you want to add. Highlighting an existing user and clicking **Delete** removes the user from the list of valid members.



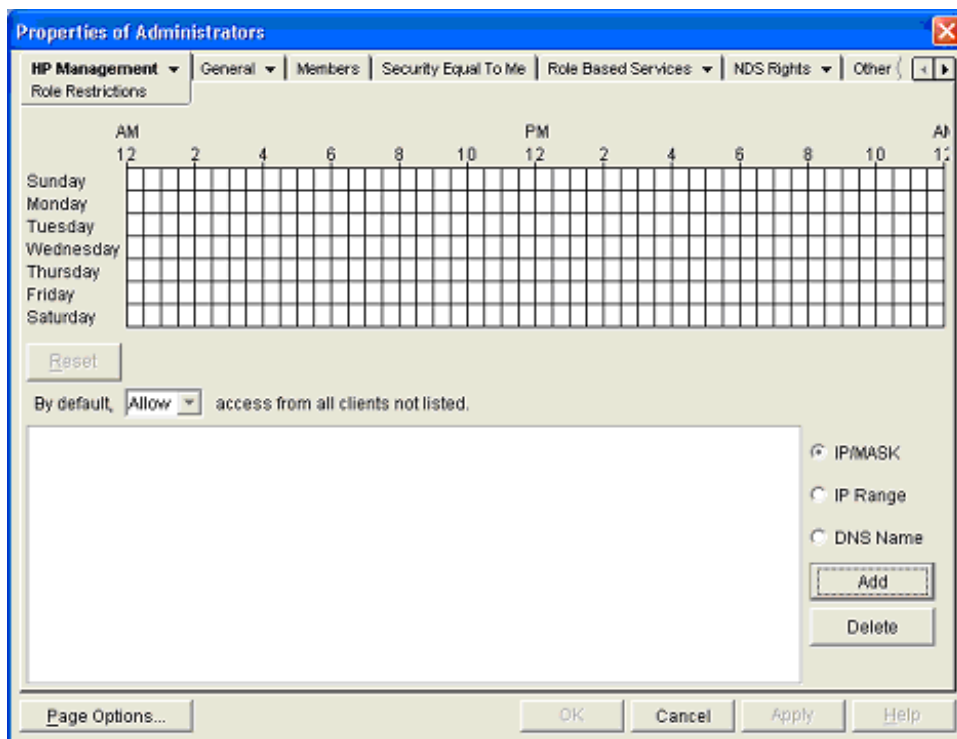
## Role Restrictions

The **Role Restrictions** subtab allows you to set login restrictions for the role. These restrictions include:

- Time Restrictions
- IP Network Address Restrictions
  - IP/Mask



- IP Range
- DNS Name



## Time Restrictions

You can manage the hours available for logon by members of the role by using the time grid displayed in the **Role Restrictions** subtab. You can select the times available for logon for each day of the week in half-hour increments. You can change a single square by clicking it, or a section of squares by clicking and holding the mouse button, dragging the cursor across the squares to be changed, and releasing the mouse button. The default setting is to allow access at all times.

## Enforced Client IP Address or DNS Name Access

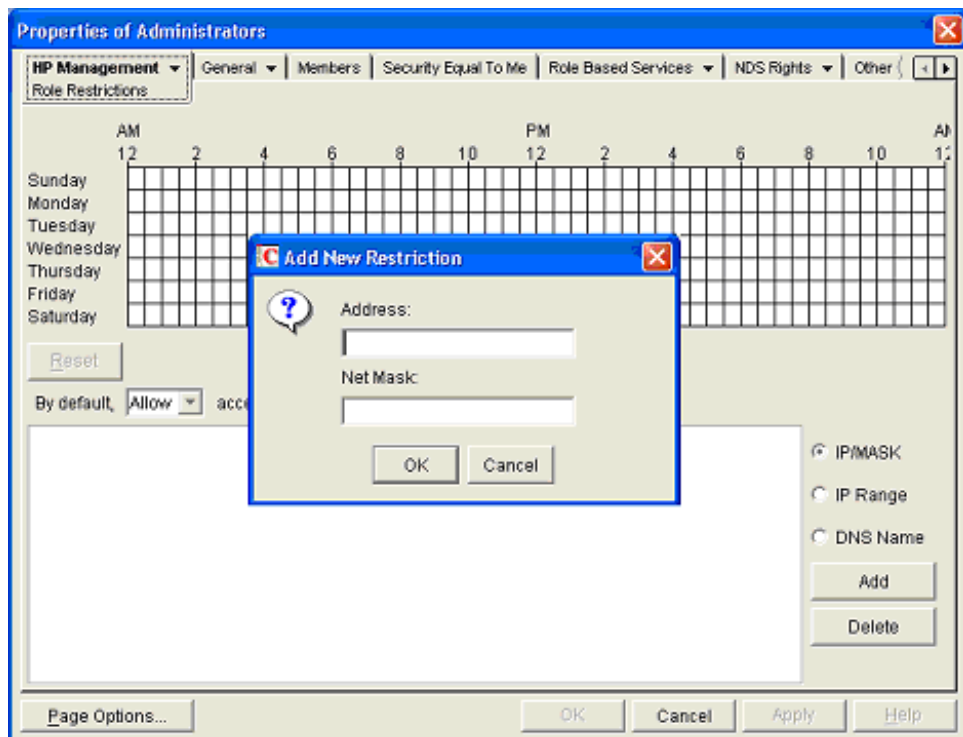
Access can be granted or denied to an IP address, IP address range, or DNS names.

1. In the **By Default** drop-down menu, select whether to **Allow** or **Deny** access from all addresses except the specified IP addresses, IP address ranges, and DNS names.
2. Select the addresses to be added, select the type of restriction, and click **Add**.
3. In the **Add New Restriction** popup window, enter the information and click **OK**. The **Add New Restriction** popup for the IP/Mask option is shown.

**NOTE:** The **DNS Name** option allows you to restrict access based on a single DNS name or a subdomain, entered in the form of host.company.com or \*.domain.company.com.

4. Click **Apply** to save the changes.

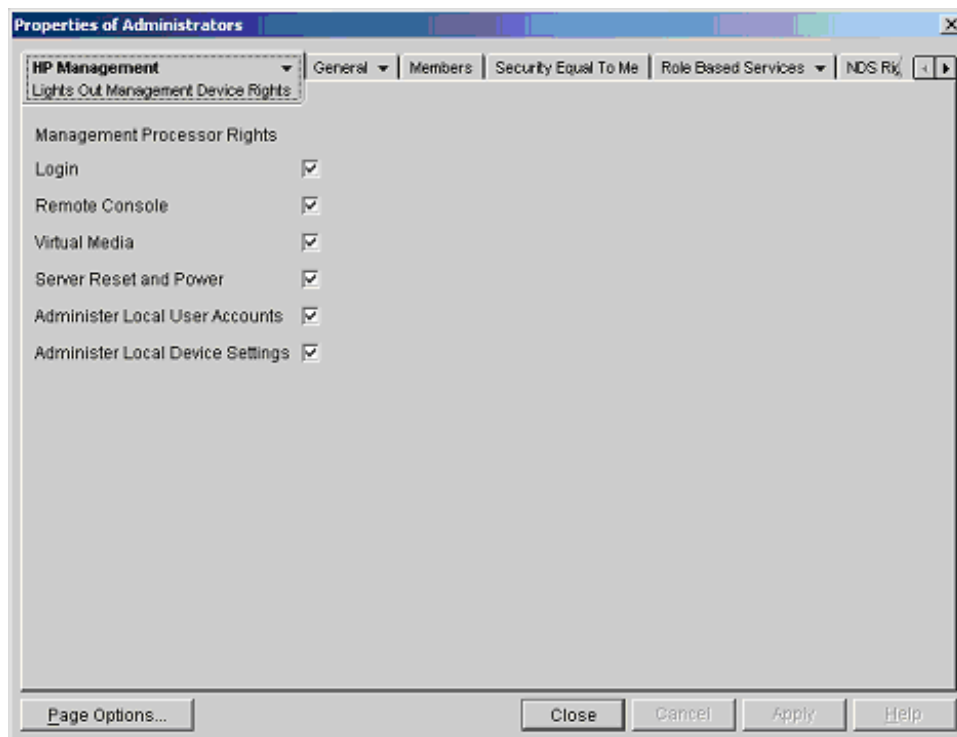
To remove any of the entries, highlight the entry in the display field and click **Delete**.



## Lights-Out Management

After a role is created, rights for the role can be selected. Users and group objects can now be made members of the role, giving the users or group of users the rights granted by the role. Rights are managed on the

**Lights Out Management Device Rights** subtab of the **HP Management** tab.



The available rights are:

- **Login**—This option controls whether users can log in to the associated devices.
- **Remote Console**—This option enables the user access to the **Remote Console**.
- **Virtual Media**—This option enables the user access to the iLO virtual media functionality.

- **Server Reset and Power**—This option enables the user access to the iLO **Virtual Power** button to remotely reset the server or power it down.
- **Administer Local User Accounts**—This option enables the user to administer accounts. The user can modify their account settings, modify other user account settings, add users, and delete users.
- **Administer Local Device Settings**—This option enables the user to configure the iLO management processor settings. These settings include the options available on the **Global Settings**, **Network Settings**, **SNMP Settings**, and **Directory Settings** screens of the iLO Web browser.

## Configuring Directory Settings

The screenshot shows the iLO Directory Settings page. At the top, the HP iLO logo and 'INTEGRATED LIGHTS-OUT' text are on the left. On the right, server information is displayed: Server Name: HP-PKXJFOR8WFDG, iLO Name: ILO0234KJ440002, and Current User: Administrator. Below this is a navigation bar with tabs: System Status, Remote Console, Virtual Devices, and Administration (selected). A link for 'Insight Agent | Log out' is on the far right. A left sidebar contains a list of settings categories: User Administration, Global Settings, Network Settings, SNMP/Insight Manager Settings, Upgrade iLO Firmware, Licensing, Certificate Administration, and Directory Settings (highlighted). The main content area is titled 'Directory Settings' with a help icon (?). It contains the following settings:

- Enable Directory Authentication: ☒ Yes ☐ No
- Enable Local User Accounts: ☐ Yes ☐ No
- Directory Server Address:
- Directory Server LDAP Port:
- LOM Object Distinguished Name:
- LOM Object Password:
- LOM Object Password Confirm:
- Directory User Context 1:
- Directory User Context 2:
- Directory User Context 3:

At the bottom of the settings area are two buttons: 'Test Settings' and 'Apply Settings'.

The **Directory Settings** screen contains the following settings options:

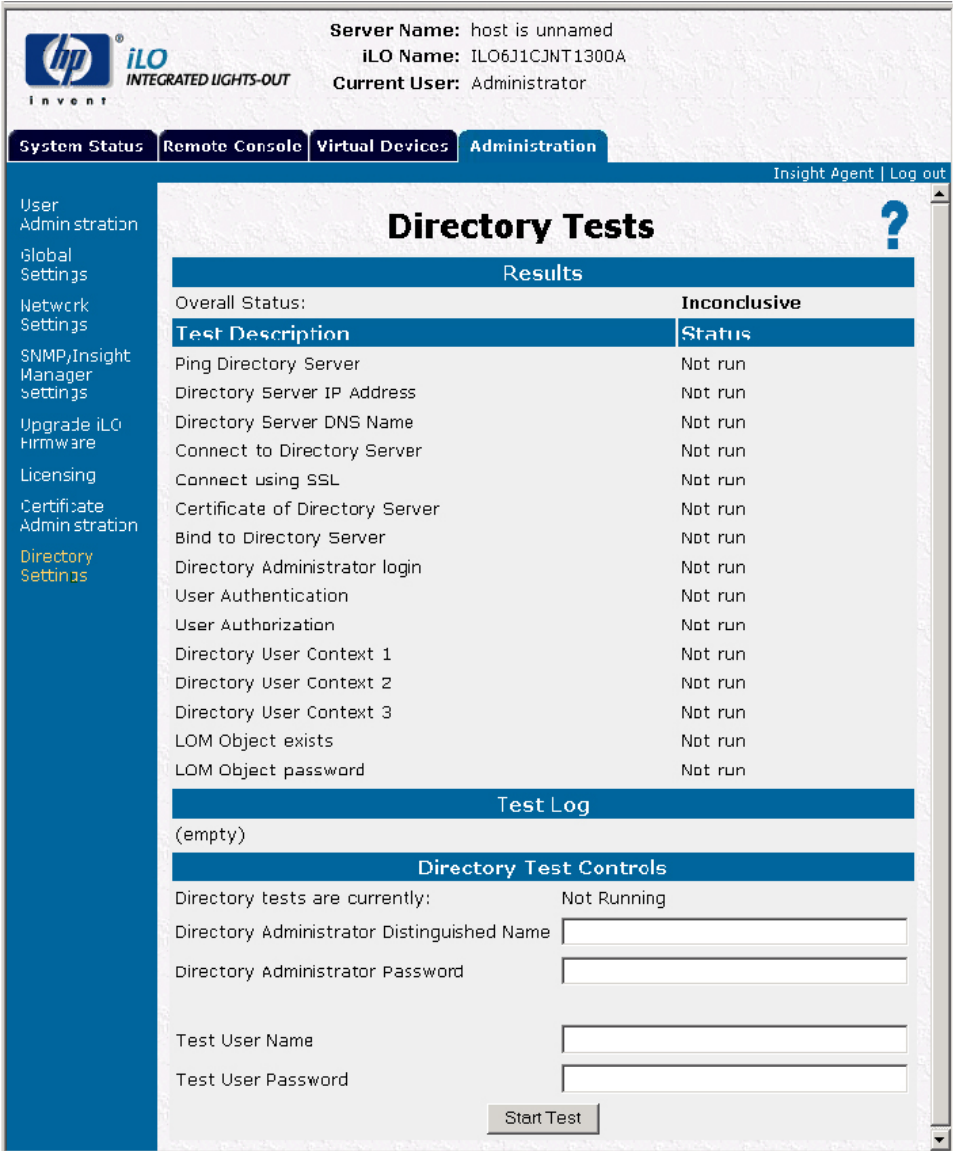
- **Directory Authentication**—This option designates whether a directory server is used to authenticate a user login. By default, this setting is **Disabled**.
- **Local User Accounts**—This options enables a user to log in using a local user account instead of a directory account. By default, this setting is **Enabled**.
- **Directory Server Address**—This option designates the IP address or DNS Name of the directory server or the name of the domain. This setting is required if you are using directory services for user authentication. HP recommends using a DNS name or multi-host DNS name. If an IP address is used, the directory will not be available if that server is down.
- **Directory Server LDAP Port**—This option designates the port used for LDAP communications. The default setting is the secure LDAP port 636. If you change the LDAP port, it must be an LDAP over SSL port.
- **LOM Object Distinguished Name**—This option specifies the full distinguished name of the Lights-Out Device object in the directory service. For example, CN=RILOE2OBJECT,CN=Users,DC=HP,DC=com. Distinguished names are limited to 256 characters.
- **LOM Object Password**—This option specifies the password the Lights-Out device object will use to login to its corresponding object in the directory. The password is used by the iLO to communicate with the directory. It is not necessary if the directory will only be used for user authentication and access. Passwords are limited to 39 characters.

**NOTE:** At this time, the LOM Object Password field is not used. This field is to provide forward compatibility with future firmware releases.
- **Directory User Context**—This option specifies search contexts when authenticating a user. These settings point to areas in the directory service where users are located so the user does not have to enter the complete tree structure when logging in. For example, CN=Users,DC=HP,DC=com. Directory User Contexts are limited to 128 characters each.

Any changes to the screen are completed by clicking **Apply Settings**. **Test Settings** enables you to test the communication between the directory server and the iLO board.

## Directory Tests

To validate current directory settings for iLO, click the **Test Settings** button on the Directory Settings page. The Directory Tests page will display.



hp iLO INTEGRATED LIGHTS-OUT  
invent

Server Name: host is unnamed  
iLO Name: ILO6J1CJNT1300A  
Current User: Administrator

System Status Remote Console Virtual Devices Administration

Insight Agent | Log out

User Administration  
Global Settings  
Network Settings  
SNMP/Insight Manager Settings  
Upgrade iLO Firmware  
Licensing  
Certificate Administration  
**Directory Settings**

### Directory Tests ?

Results	
Test Description	Status
Overall Status:	Inconclusive
Ping Directory Server	Not run
Directory Server IP Address	Not run
Directory Server DNS Name	Not run
Connect to Directory Server	Not run
Connect using SSL	Not run
Certificate of Directory Server	Not run
Bind to Directory Server	Not run
Directory Administrator login	Not run
User Authentication	Not run
User Authorization	Not run
Directory User Context 1	Not run
Directory User Context 2	Not run
Directory User Context 3	Not run
LOM Object exists	Not run
LOM Object password	Not run

### Test Log

(empty)

### Directory Test Controls

Directory tests are currently: Not Running

Directory Administrator Distinguished Name

Directory Administrator Password

Test User Name

Test User Password

Start Test

The test page displays the results of a series of simple tests designed to validate the current directory settings. Additionally, it includes a test log that shows test results as well as any problems that have been detected. After your directory settings are configured correctly, you do not need to re-run these tests. The Directory Tests screen does not require the user to be logged-in as a directory user.

To verify your directory settings, enter the distinguished name and password of a directory administrator. A good choice would be the same credentials used when creating the iLO objects in the directory. These credentials are not stored by iLO. They are used to verify the iLO object and user search contexts.

Also enter a test user name and password. Typically, this would be an account intended to access the iLO being tested. It can be the same account as the directory administrator, however the tests will be unable to verify user authentication with a "superuser" account. These credentials are not stored by iLO.

After pressing the **Start Test** button, several tests begin in the background, starting with a network ping of the directory user through establishing an SSL connection to the server and evaluating user privileges as they would be evaluated during a normal login.

While the tests are running, the page periodically refreshes. At any time during test execution, you can stop the tests or manually refresh the page.

Consult the help link on the page for test details and actions in the event of trouble.

## User Login to iLO

The iLO login page **Login Name** field accepts all of the following:

- Directory users
- LDAP Fully Distinguished Names

Example: CN=John Smith,CN=Users,DC=HP,DC=COM, or @HP.com

**NOTE:** The short form of the login name by itself does not tell the directory which domain you are trying to access. You must provide the domain name or use the LDAP distinguished name of your account.

- DOMAIN\user name form (Active Directory Only)

Example: HP\jsmith

- username@domain form (Active Directory Only)

Example: jsmith@hp.com

**NOTE:** Directory users specified using the @ searchable form may be located in one of three searchable contexts, which are configured within **Directory Settings**.

- User name form

Example: John Smith

**NOTE:** Directory users specified using the user name form may be located in one of three searchable contexts, which are configured within **Directory Settings**.

- Local users—Login-ID

**NOTE:** On the iLO login page, the maximum length of the **Login Name** is 39 characters for local users. For Directory Services users, the maximum length of the **Login Name** is 256 characters.

The local user database is retained. The customer can decide not to use directories, to use a combination of directories and local accounts, or use directories exclusively for authentication.

**NOTE:** When connected through the Diagnostics Port, the directory server is not available. You can log in using a Local account only.



---

# Group Administration and Integrated Lights-Out Scripting

## In This Section

Features of the Lights-Out Configuration Utility .....	141
Group Administration Using the Lights-Out Configuration Utility and Insight Manager 7	142
Batch Processing Using the Lights-Out Configuration Utility .....	145

## Features of the Lights-Out Configuration Utility

Firmware version 1.10 added support for XML-based scripted configuration of iLO. User Administration, Global Settings, Network Settings, SNMP/Insight Manager Settings, Upgrade iLO Firmware, Licensing, and ProLiant BL p-Class Rack Settings may be configured through iLO scripting.

The scripting utility that can be used for iLO is the Lights-Out Configuration Utility (CPQLOCFG.EXE), which is a Windows-based utility that connects to iLO using a secure connection over the network. This utility may be downloaded from the HP website (<http://www.hp.com/servers/lights-out>).

The CPQLOCFG utility may be launched from Insight Manager 7 for Group Administration or used independently for a command prompt for batch processing.

**NOTE:** Version 2.2 of CPQLOCFG.EXE is required to configure the iLO Directory Settings XML script.

The Lights-Out Configuration Utility allows you to perform the following functions:

- Add, modify, or delete a user.
- Obtain individual or all users' configuration information.
- Modify network settings.
- Modify global settings.

- Modify directory settings.
- Clear the iLO Event Log.
- Obtain the firmware version of the iLO.
- Update the iLO firmware.
- Configure Remote Console hot key settings.
- Obtain and set Virtual Power Button status.
- Obtain the server power status.
- Reset the server.

## Group Administration Using the Lights-Out Configuration Utility and Insight Manager 7

After the firmware has been updated, the IT administrator can manage multiple iLO processors through Insight Manager 7. The four components of Group Administration are RIBCL, the Lights-Out Configuration Utility, Query Definition in Insight Manager 7, and Application Launch.

Insight Manager 7 discovers the iLO devices as management processors. Insight Manager 7 uses the Lights-Out Configuration Utility to send an RIBCL file to a group of iLO processors to manage the user accounts for those iLO processors. The iLO processors then perform the action designated by the RIBCL file and send a response to the log file.

### Lights-Out Configuration Utility

The Lights-Out Configuration Utility is used to execute RIBCL scripts on the iLO boards. The executable file for the utility is CPQLOCFG.EXE. You can download this utility from the HP website (<http://www.hp.com/servers/lights-out>).

The Lights-Out Configuration Utility must reside on the same server as Insight Manager 7. The Lights-Out Configuration Utility generates two types of error messages: runtime and syntax. A runtime error occurs when an invalid action is requested.

**NOTE:** Runtime errors are logged to the following directory:  
C:\PROGRAM FILES\INSIGHT MANAGER 7

A syntax error occurs when an invalid XML tag is encountered. When a syntax error occurs, the Lights-Out Configuration Utility stops running and logs the error in the runtime script and output log file.

**NOTE:** Syntax errors take the format of "Syntax error: expected 'x' but found 'y' " as shown in the following example: Syntax error:  
expected USER\_LOGIN=userlogin but found  
USER\_NAME=username

Refer to the RIBCL section ("Remote Insight Command Language" on page 159) for a complete listing of errors.

## Query Definition in Insight Manager 7

To group all of the iLO boards, log in to Insight Manager 7 and create a query.

To create the query:

1. Log in to Insight Manager 7.
2. Click **Device** in the navigation bar on the top left side of the screen.
3. Click **Queries**, then click **Device**.
4. Locate the **Personal Queries** section in the main window. If a query category exists, proceed to step 7; otherwise proceed to step 5.
5. Click **New** to create a new category. For this example, the name of the new category is RIB Cards. Click **Create Category**.
6. Click **Queries** to return to the **Device Queries** screen.
7. Click **New**, within the appropriate query category, to open the **Create/Edit Query** screen where the query definition is created.
8. Define the query name, for example "Mgmt Processors."
9. Select **Device(s) of type** and then select **Devices by product name**. In the criteria windows, set the product name to **Integrated Lights-Out**.
10. Click **type** in the **Query Description** field. A popup window opens where you define the device type.

11. Select **Management Processor** and click **OK**.
12. Click **Save** to return to the **Device Query** screen.
13. Find the newly created query in the appropriate query category and click the query name to run it for verification.
14. Click **Overview** on the left side of the screen after the verification has taken place. The initial page for devices opens.

## Application Launch Using Insight Manager 7

The application launch combines the RIBCL, the Lights-Out Configuration Utility, and the query definition to manage the Group Administration for the iLO management processors.

To create an Application Launch task:

1. Click **Device** in the navigation bar on the top left side of the screen.
2. Click **Tasks** to open the **Tasks** screen.
3. Click **New Control Task**. A drop-down menu is displayed.
4. Click **Application Launch** from the drop-down menu to open the **Create/Edit Task** screen.
5. Enter the full path and name for the Lights-Out Configuration Utility in the area provided. If the CPQLOCFG.EXE file is in the root directory of the C:\ drive, then the path is: C:\cpqlocfg.exe.
6. Enter the parameters in the area provided. Insight Manager 7 requires the following parameters for the Lights-Out Configuration Utility:
  - F is the full path of the RIBCL file name.
  - V is the verbose message (optional).

If the RIBCL file is in the root directory of on the C:\ drive, then the parameters are:

```
-F C:\MANAGEUSERS.xml -V
```

**NOTE:** Insight Manager 7 does not allow the `-L` parameter to designate an output log file. A default log file named with the DNS name or the IP address is created in the same directory where CPQLOCFG is launched.

7. Click **Next**. A screen is displayed with options for naming the task, defining the query association, and setting a schedule for the task.
8. Enter a task name in the **Enter a name for this task** field.
9. Select the query that had been created earlier, for example "Mgmt Processors."
10. Click **Schedule** to define when the Application Launch task will run. A schedule configuration window is displayed.
11. Click **OK** to set the schedule.

**NOTE:** The default schedule for a control task is **Now**.

12. Click **Finish** to save the Application Launch task.
13. Click the **Execute a Task** icon (the green triangle) to execute the Group Administration.

**NOTE:** Insight Manager 7 does not allow the `-L` parameter to designate an output log file. A default log file named with the DNS name or the IP address is created in the same directory where CPQLOCFG is launched.

**NOTE:** Syntax errors take the format of "Syntax error: expected 'x' but found 'y' " as shown in the following example: Syntax error:  
expected USER\_LOGIN=userlogin but found  
USER\_NAME=username

## Batch Processing Using the Lights-Out Configuration Utility

Group Administration can also be delivered to iLO through batch processing. The components used by batch processing are the Lights-Out Configuration Utility, an RIBCL file, and a batch file.

## Lights-Out Configuration Utility Parameters

The Lights-Out Configuration Utility is used to execute the RIBCL ("Remote Insight Command Language" on page 159) on the Integrated Lights-Out. The executable for the Lights-Out Configuration Utility is CPQLOCFG.EXE. This utility can be downloaded from the HP website (<http://www.hp.com/servers/lights-out>).

The following example shows a sample batch file that can be used to perform the Group Administration for the Integrated Lights-Out:

```
REM Updating the Integrated Lights-Out board
REM Repeat line for each board to be updated
REM
CPQLOCFG -S RIB1 -F C:\...SCRIPT.XML -L RIB1LOG.TXT -V
CPQLOCFG -S RIB2 -F C:\...SCRIPT.XML -L RIB2LOG.TXT -V
CPQLOCFG -S RIB3 -F C:\...SCRIPT.XML -L RIB3LOG.TXT -V
.
.
.
CPQLOCFG -S RIBN -F C:\...SCRIPT.XML -L LOGFILE.TXT -V
```

- -S is the switch that determines the Integrated Lights-Out that is to be updated. This switch is either the DNS name or IP address of the target server.

Do **not** use this switch if you are launching from iLO. Insight Manager 7 will provide the address of the Insight Manager 7 when CPQLOCFG.EXE is launched.

- -F is the switch that gives the full path location and name of the RIBCL file that contains the actions to be performed on the board.
- -L is the switch that defines where the log file will be generated and what the file name will be. If this switch is omitted, a default log file with the DNS name or the IP address is created in the same directory used to launch CPQLOCFG.

Do **not** use this switch if launching from Insight Manager 7.

- -V is the optional switch that turns on the verbose message return. The resulting log file contains all commands sent to the Remote Insight board, all responses from the Remote Insight board, and any errors. By default, only errors and responses from GET commands are logged without this switch.

- `-C` causes CPQLOCFG to check the syntax of the XML, but not open a connection to the Remote Insight board.

The switches `-L` and `-V` may or may not be set depending on the IT administrator's preferences.

If it is not in the same directory, be sure that the Lights-Out Configuration Utility is in a directory referenced by the `PATH` environment variable. Any log files generated are placed in the same directory as the Lights-Out Configuration Utility executable.

**NOTE:** The Lights-Out Configuration Utility overwrites any existing log files.

# Lights-Out DOS Utility

## In This Section

Overview of the Lights-Out DOS Utility .....	149
CPQLODOS General Guidelines .....	150
Command Line Arguments .....	150
CPQLODOS .....	152
MOD_NETWORK_SETTINGS .....	152
MOD_DIR_CONFIG .....	155
ADD_USER .....	157

## Overview of the Lights-Out DOS Utility

CPQLODOS is a command line utility that is a part of the SmartStart Scripting Toolkit. It is intended to be an initial configuration program to set up only those essential iLO settings necessary to allow one of the other full-featured configuration methods. Because of this limited usage model, it processes only a small subset of the iLO scripting language.

**NOTE:** CPQLODOS is a DOS-only tool that requires MS-DOS® 6.0 or higher. Lights-Out scripting is not supported on Linux operating systems or when using the Novell NetWare Client.

CPQLODOS enables you to configure features exposed through F8 startup or the graphical user interface. This utility is not intended for continued administration. The RIBCL should be used to administer user rights and network functionality on the server.

**NOTE:** This utility is primarily a reconfiguration tool. Any existing configuration will be removed.



## CPQLODOS General Guidelines

In this section, all of the commands are grouped by functionality. All commands that manipulate user information are grouped together. Grouping commands allows the firmware to view the data to be manipulated as a block of information, similar to a text document, allowing for multithreaded access to the different kinds of information.

An opening command opens a database. The database remains open until the matching closing command is sent. All changes made within a single command block are applied simultaneously when the database is closed. Any errors within the block cause the enclosed changes to be discarded.

An example of an opening command and its matching closing command are as follows:

```
<USER_INFO>  
</USER_INFO>
```

In all examples, the opening and closing commands are displayed.

## Command Line Arguments

The following table lists the arguments recognized by CPQLODOS.

<b>Command Line Argument</b>	<b>Description</b>
/HELP or /?	These arguments display simple help messages.
/RESET_RILOE	This argument resets the iLO management processor to default factory settings.
/DETECT	This argument detects the iLO management processor on the target server.
/RESET_RILOE	This argument resets the iLO management processor.
/VIRT_FLOPPY	This argument ignores the virtual floppy inserted error.
/MIN_FW-xxx	This argument enables you to set the minimum firmware version on which the iLO management processor runs.
/GET_STATUS	This argument returns the status of the iLO management processor.
/GET_HOSTINFO	This argument retrieves and displays the current host server information on the iLO management processor and displays the server name and number.
/GET_USERINFO	This argument obtains the current users stored in the iLO management processor board and displays the names, login names, and security mask information.
/GET_NICCONFIG	This argument retrieves and displays the NIC settings stored in the iLO management processor.
/GET_DHCPCONFIG	This argument retrieves and displays the DHCP settings stored in the iLO management processor.
/GET_DIRCONFIG	This argument retrieves and displays the DIRECTORY settings in the iLO management processor.
/WRITE_XML=A:\DL360.RLO	This argument reads the settings on the iLO management processor and writes the NIC, DHCP, DIRECTORY, and user settings into an XML hardware configuration script file.
/LOAD_XML=A:\DL360.RLO	This argument loads the script file and applies its changes to the current configuration on the iLO management processor.
/VERIFY_XML	This argument verifies the accuracy of the script file and generates an error message for any incorrect data.

CPQLODOS processes the <CPQLODOS>, the <MOD\_NETWORK\_SETTINGS>, the <MOD\_DIR\_CONFIG>, and the <ADD\_USER> XML scripting language blocks. Only those parameters referenced in the following sections are supported.

## CPQLODOS

This command is used to start and end a CPQLODOS session. It can be used only once, and it must be the first and last statement in an XML script.

Example:

```
<CPQLODOS VERSION="2.0">
</CPQLODOS>
```

### CPQLODOS Parameter

VERSION is a numeric string that indicates the version of CPQLODOS necessary to process this script. The VERSION string is compared to the version that CPQLODOS can process. An error is returned if the version of CPQLODOS and the version of the script do not match. The VERSION parameter can never be blank.

### CPQLODOS Runtime Error

The possible CPQLODOS error messages include `Version must not be blank`.

## MOD\_NETWORK\_SETTINGS

This command modifies certain network settings. All of the elements are optional and any options not specified will be set to the factory default.

Example:

```
<MOD_NETWORK_SETTINGS>
  <SPEED_AUTOSELECT VALUE = "N"/>
  <NIC_SPEED VALUE = "10"/>
```

```

<FULL_DUPLEX VALUE = "N"/>
<IP_ADDRESS VALUE = "192.168.1.2"/>
<SUBNET_MASK VALUE = "255.255.255.0"/>
<GATEWAY_IP_ADDRESS VALUE = "192.168.1.222"/>
<DNS_NAME VALUE = "RIB0002A5617D3B"/>
<PRIM_DNS_SERVER value = "192.168.2.200"/>
<DOMAIN_NAME VALUE = "riloe.mgmt.net"/>
<DHCP_ENABLE VALUE = "Y"/>
<DHCP_GATEWAY VALUE = "Y"/>
<DHCP_DNS_SERVER VALUE = "Y"/>
<DHCP_STATIC_ROUTE VALUE = "Y"/>
<DHCP_WINS_SERVER VALUE = "Y"/>
<REG_WINS_SERVER VALUE = "Y"/>
<PRIM_WINS_SERVER VALUE = "192.168.2.220"/>
<STATIC_ROUTE_1 DEST = "192.168.5.1" GATEWAY =
"192.168.5.200"/>
<STATIC_ROUTE_2 DEST = "192.168.5.2" GATEWAY =
"192.168.5.200"/>
<STATIC_ROUTE_3 DEST = "192.168.5.3" GATEWAY =
"192.168.5.200"/>
</MOD_NETWORK_SETTINGS>

```

## MOD\_NETWORK\_SETTINGS Parameters

**SPEED\_AUTOSELECT** is used to automatically select the transceiver speed. The possible values are "Yes" or "No." It is case insensitive.

**FULL\_DUPLEX** is used to decide if the iLO is to support full-duplex or half-duplex mode. It is only applicable if **SPEED\_AUTOSELECT** was set to "No." The possible values are "Yes" or "No." It is case insensitive.

**NIC\_SPEED** is used to set the transceiver speed if **SPEED\_AUTOSELECT** was set to "No." The possible values are "10" or "100." Any other values will result in a syntax error.

**DHCP\_ENABLE** is used to enable DHCP. The possible values are "Yes" or "No." It is case insensitive.

**IP\_ADDRESS** is used to select the IP address for the iLO if DHCP is not enabled. If an empty string is entered, the current value is deleted.

SUBNET\_MASK is used to select the subnet mask for the iLO if DHCP is not enabled. If an empty string is entered, the current value is deleted.

GATEWAY\_IP\_ADDRESS is used to select the default gateway IP address for the iLO if DHCP is not enabled. If an empty string is entered, the current value is deleted.

DNS\_NAME is used to specify the DNS name for the iLO. If an empty string is entered, the current value is deleted.

DOMAIN\_NAME is used to specify the domain name for the network where the iLO resides. If an empty string is entered, the current value is deleted.

DHCP\_GATEWAY specifies if the DHCP-assigned gateway address is to be used. The possible values are "Yes" or "No." It is case sensitive. This selection is only valid if DHCP is enabled.

DHCP\_DNS\_SERVER specifies if the DHCP-assigned DNS server is to be used. The possible values are "Yes" or "No." It is case sensitive. This selection is only valid if DHCP is enabled.

DHCP\_WINS\_SERVER specifies if the DHCP-assigned WINS server is to be used. The possible values are "Yes" or "No." It is case sensitive. This selection is only valid if DHCP is enabled.

DHCP\_STATIC\_ROUTE specifies if the DHCP-assigned static routes are to be used. The possible values are "Yes" or "No." It is case sensitive. This selection is only valid if DHCP is enabled.

REG\_WINS\_SERVER specifies if the iLO needs to register with the WINS server. The possible values are "Yes" or "No." It is case sensitive. This selection is only valid if DHCP is enabled.

PRIM\_DNS\_SERVER specifies the IP address of the primary DNS server. This parameter is only relevant if the DHCP-assigned DNS server address feature is disabled. If an empty string is entered, the current value is deleted.

SEC\_DNS\_SERVER specifies the IP address of the secondary DNS server. This parameter is only relevant if the DHCP-assigned DNS server address feature is disabled. If an empty string is entered, the current value is deleted.

TER\_DNS\_SERVER specifies the IP address of the tertiary DNS server. This parameter is only relevant if the DHCP-assigned DNS server address feature is disabled. If an empty string is entered, the current value is deleted.

PRIM\_WINS\_SERVER specifies the IP address of the primary WINS server. This parameter is only relevant if the DHCP-assigned WINS server address feature is disabled. If an empty string is entered, the current value is deleted.

SEC\_WINS\_SERVER specifies the IP address of the secondary WINS server. This parameter is only relevant if the DHCP-assigned WINS server address feature is disabled. If an empty string is entered, the current value is deleted.

STATIC\_ROUTE\_1, STATIC\_ROUTE\_2, and STATIC\_ROUTE\_3 are used to specify the destination and gateway IP addresses of the static routes. The following two parameters are used within the static route commands. If an empty string is entered, the current value is deleted.

- DEST specifies the destination IP addresses of the static route. This parameter is only relevant if the DHCP-assigned static route feature is disabled. If an empty string is entered, the current value is deleted.
- GATEWAY specifies the gateway IP addresses of the static route. This parameter is only relevant if the DHCP-assigned static route feature is disabled. If an empty string is entered, the current value is deleted.

**NOTE:** The iLO is rebooted to apply the changes after MOD\_NETWORK\_SETTINGS has been closed.

## MOD\_DIR\_CONFIG

This command will modify certain directory services settings. If directory services is enabled, then all of the mandatory parameters must be entered for successful operation of directory services authentication and authorization.

Example:

```
<MOD_DIR_CONFIG>
  <DIR_AUTHENTICATION_ENABLED VALUE = " YES"/>
  <DIR_LOCAL_USER_ACCT VALUE = "YES"/>
  <DIR_SERVER_ADDRESS VALUE = "\"directory.corp.net\""/>
  <DIR_SERVER_PORT VALUE = "636"/>
```

```
<DIR_OBJECT_DN VALUE = "CN=RILOE2-JJ, OU=RILOES,  
DC=RILOEII, DC=HP"/>  
<DIR_OBJECT_PASSWORD VALUE = "wingsauce"/>  
<DIR_USER_CONTEXT_1 VALUE = "CN=Users, DC=RILOEII,  
DC=HP"/>  
<DIR_USER_CONTEXT_2 VALUE = "CN=Mgmt, DC=RILOEII,  
DC=HP"/>  
<DIR_USER_CONTEXT_3 VALUE = "CN=Admins, DC=RILOEII,  
DC=HP"/>  
</MOD_DIR_CONFIG>
```

## MOD\_DIR\_CONFIG Parameters

DIR\_AUTHENTICATION\_ENABLED indicates if directory services should be used to determine authentication to and authorization for the iLO. The possible values are "Y," "Yes," "N," or "No." The default value is "No." This parameter is optional.

DIR\_LOCAL\_USER\_ACCT indicates if the local user accounts should be used in addition to using directory services user accounts. The possible values are "Y," "Yes," "N," or "No." It is effective only if

DIR\_AUTHENTICATION\_ENABLED is set to **Yes**. The default value is "Yes." This parameter is optional.

DIR\_SERVER\_ADDRESS specifies the IP address or DNS name of the computer that the iLO will use for directory services operations. The possible values are a string or an IP address. This parameter is mandatory if DIR\_AUTHENTICATION\_ENABLED is set to **Yes**.

DIR\_SERVER\_PORT specifies what port number on the directory services server that the iLO will use for communication. The possible values are any valid numeric IP port number. The default value is 636 and is an optional parameter.

DIR\_OBJECT\_DN\_VALUE specifies the directory services distinguished name of the iLO object in the directory. The possible value is a string that is the appropriate distinguished name of the iLO. This parameter is mandatory if DIR\_AUTHENTICATION\_ENABLED is set to **Yes**.

DIR\_OBJECT\_PASSWORD specifies a password for the iLO that is used to access iLO objects. This password is currently unused but will be used in a future version of the firmware.

DIR\_USER\_CONTEXT\_1, DIR\_USER\_CONTEXT\_2, and DIR\_USER\_CONTEXT\_3 specify directory service contexts that will be searched in the authentication and authorization process. When attempting to access a directory service, the user's name is added in front of each context string to form the full user name that is authenticated with directory services. The possible values are any valid directory service context string. These parameters are optional.

## ADD\_USER

This command is used to add a user to the iLO. If there are multiple ADD\_USER commands in the XML script, CPQLODOS will use only the settings from the last command.

Example:

```
<ADD_USER
  USER_NAME = "James Madison"
  USER_LOGIN = "jmadison"
  PASSWORD = "president">
</ADD_USER>
```

## ADD\_USER Parameters

USER\_NAME is the actual name of the user to be added. This parameter is case sensitive, can be any valid string, and has a maximum length of 39 characters. This string is used for display only and must never be blank.

USER\_LOGIN is the name that the user types in to log in to iLO. This parameter is case sensitive, can be any valid string, and has a maximum length of 39 characters. The string must never be blank.

PASSWORD is the password that will be associated with the user. This parameter has a minimum length of 0 characters, a maximum length of 39 characters, depending on the minimum password length set on the Global Settings screen. PASSWORD is an ASCII string that may contain any combination of printable characters. The PASSWORD parameter cannot contain both single and double quote characters. This parameter is case sensitive.



# Remote Insight Command Language

## In This Section

Overview of the Remote Insight Board Command Language.....	160
RIBCL Sample Scripts .....	160
RIBCL General Guidelines .....	160
XML Header.....	161
Data Types.....	161
Response Definitions.....	162
RIBCL .....	162
LOGIN.....	163
USER_INFO.....	164
ADD_USER .....	165
DELETE_USER.....	168
GET_USER .....	169
MOD_USER.....	171
GET_ALL_USERS .....	173
GET_ALL_USER_INFO .....	175
RIB_INFO .....	176
RESET_RIB .....	177
GET_NETWORK_SETTINGS.....	177
MOD_NETWORK_SETTINGS .....	179
MOD_DIAGPORT_SETTINGS .....	183
DIR_INFO .....	184
GET_DIR_CONFIG.....	185
MOD_DIR_CONFIG .....	186
GET_GLOBAL_SETTINGS .....	188
MOD_GLOBAL_SETTINGS .....	189
MOD_SNMP_IM_SETTINGS .....	190
CLEAR_EVENTLOG.....	192
UPDATE_RIB_FIRMWARE .....	193
GET_FW_VERSION .....	194
HOTKEY_CONFIG.....	195
LICENSE.....	197
RACK_INFO.....	198
MOD_BLADE_RACK .....	199
GET_TOPOLOGY .....	200

SERVER_INFO .....	201
GET_HOST_POWER_STATUS .....	202
SET_HOST_POWER.....	203
RESET_SERVER.....	204
GET_UID_STATUS .....	205
UID_CONTROL .....	205

## Overview of the Remote Insight Board Command Language

The Remote Insight Board Command Language enables you to write scripts to manage user accounts and to configure settings.

**IMPORTANT:** Comments should not interrupt a command. If they do, an error message will be generated.

## RIBCL Sample Scripts

Sample scripts for all iLO commands, described in this section are available for download from the HP website (<http://www.hp.com/servers/lights-out>).

## RIBCL General Guidelines

In this section, all of the commands are grouped by functionality. All commands that manipulate user information are grouped together. Grouping commands allows the firmware to view the data to be manipulated as a block of information, similar to a text document, allowing for multithreaded access to the different kinds of information.

An opening command opens a database. The database remains open until the matching closing command is sent. All changes made within a single command block are applied simultaneously when the database is closed. Any errors within the block cause the enclosed changes to be discarded.

An example of an opening command and its matching closing command are as follows:

```
<USER_INFO>
```

```
</USER_INFO>
```

In all examples, the opening and closing commands are displayed.

## XML Header

The XML header ensures the connection is an XML connection, not an HTTP connection. The XML header is built into the cpqlocfg utility and has the following format:

```
<?xml version="1.0"?>
```

## Data Types

The three data types that are allowed in the parameter are:

- String
- Specific string
- Boolean string

### String

A string is any text enclosed in quotes. It can include spaces, numbers, or any printable character. A string may start with either a double or single quote and it must end with the same type of quote. The string may contain a quote if it is different from the string delimiter quotes.

For example, if a string is started with a double quote, a single quote can be used within the string and the string must be closed with a double quote.

### Specific String

A specific string is one that is required to contain certain characters. In general, you have a choice of words that are accepted as correct syntax and all other words produce an error.

## Boolean String

A Boolean string is a specific string that specifies a "yes" or "no" condition. Acceptable Boolean strings are "yes," "y," "no," "n," "true," "t," "false," and "f." These strings are not case sensitive.

## Response Definitions

Every command that is sent to iLO generates a response. The response indicates whether the command succeeded or failed. Some commands generate additional information. The additional information is displayed in execution sequence, provided that no error occurred.

Example:

```
<RESPONSE
  STATUS="0x0001"
  MSG="There has been a severe error."
/>
```

- **RESPONSE**

This tag name indicates that iLO is sending a response to the previous commands back to the client application to indicate the success or failure of the commands that have been sent to iLO.

- **STATUS**

This parameter contains an error number. The number "0x0000" indicates that there is no error.

- **MSG**

This element contains a message describing the error that happened. If no error occurred, the message "No error" is displayed.

## RIBCL

This command is used to start and end an RIBCL session. You can use it only once to start an RIBCL session, and it must be the first command to display in the script. The RIBCL tags are required to mark the beginning and the end of the RIBCL document.

Example:

```
<RIBCL VERSION="2.0">  
</RIBCL>
```

## RIBCL Parameter

VERSION is a string that indicates the version of the RIBCL that the client application is expecting to use. The VERSION string is compared to the version of the RIBCL that is expected, and an error is returned if the string and the version do not match. The preferred value for the VERSION parameter is "2.0." The VERSION parameter is no longer checked for an exact match; however, this parameter can never be blank.

## RIBCL Runtime Errors

The possible RIBCL error messages include:

Version must not be blank.

## LOGIN

The LOGIN command provides the information that is used to authenticate the user whose permission level will be used when performing RIBCL actions. The specified user must have at least login privilege in order to be validated to execute any RIBCL commands. The user privilege is checked against the required privilege for a particular command, and an error is returned if the privilege level does not match.

Example:

```
<LOGIN USER_LOGIN="username" PASSWORD="password">  
</LOGIN>
```

**NOTE:** Users without administrative privileges can change their password setting.

## LOGIN Parameters

USER\_LOGIN is the name that the user types in to log in to iLO. This parameter is case sensitive, can be any valid string, and has a maximum length of 39 characters. The string must never be blank.

PASSWORD is the password that will be associated with the user. This parameter has a minimum length of 0 characters, a maximum length of 39 characters, depending on the minimum password length set on the Global Settings screen. PASSWORD is an ASCII string that may contain any combination of printable characters. The PASSWORD parameter cannot contain both single and double quote characters. This parameter is case sensitive.

## LOGIN Runtime Errors

The possible runtime error messages include:

- User login name was not found.
- Password must not be blank.
- Logged-in user does not have required privilege for this command.

## USER\_INFO

The USER\_INFO command may only display within a LOGIN command. When the command is parsed, it reads the local user information database into memory and prepares to edit it. Only commands that are USER\_INFO type commands are valid inside the USER\_INFO block. The USER\_INFO command generates a response that indicates to the host application whether the user information was successfully read or not. If the user information is open for writing by another application, then this call will fail.

Example:

```
<USER_INFO MODE="write">
</USER_INFO>
```

## USER\_INFO Parameter

MODE is a specific string parameter with a maximum length of 10 characters that specifies what you intend to do with the user information. Valid arguments are "read" and "write."

If the parameter is open in write mode, then both reading and writing are enabled and other users are unable to open the user information. If it is open in read mode, then user data is not modifiable. The argument is not case sensitive. This parameter must never be blank.

## USER\_INFO Runtime Error

A possible runtime error message is: Mode parameter must not be blank.

## ADD\_USER

The ADD\_USER command is used to add a local user. All of the attributes that pertain to the user are set using the following parameters. For this command to work, the user must not already exist. Use the MOD\_USER command to change an existing user's information. The ADD\_USER command must be displayed within a USER\_INFO element, and USER\_INFO must be in write mode. The user must have administrative privilege to add other users.

```
<RIBCL VERSION="2.0">
  <LOGIN USER_LOGIN="loginname" PASSWORD="password">
    <USER_INFO MODE="write">
      <ADD_USER
        USER_NAME="User"
        USER_LOGIN="username" PASSWORD="password">
        <ADMIN_PRIV value ="No"/>
        <REMOTE_CONS_PRIV value ="Yes"/>
        <RESET_SERVER_PRIV value ="No"/>
        <VIRTUAL_MEDIA_PRIV value ="No"/>
        <CONFIG_ILO_PRIV value ="No"/>
      </ADD_USER>
    </USER_INFO>
  </LOGIN>
</RIBCL>
```

## ADD\_USER Parameters

USER\_NAME is the actual name of the user to be added. This parameter is case sensitive, can be any valid string, and has a maximum length of 39 characters. This string is used for display only and must never be blank.

USER\_LOGIN is the name that the user types in to log in to iLO. This parameter is case sensitive, can be any valid string, and has a maximum length of 39 characters. The string must never be blank.

PASSWORD is the password that will be associated with the user. This parameter has a minimum length of 0 characters, a maximum length of 39 characters, depending on the minimum password length set on the Global Settings screen. PASSWORD is an ASCII string that may contain any combination of printable characters. The PASSWORD parameter cannot contain both single and double quote characters. This parameter is case sensitive.

ADMIN\_PRIV is a Boolean parameter that allows the user to administer user accounts. The user can modify their account settings, modify other user account settings, add users, and delete users. Leaving out this parameter prevents the user from adding, deleting, or configuring accounts.

REMOTE\_CONS\_PRIV is a Boolean parameter that gives permission for the user to access the Remote Console functionality. This parameter is optional, and the Boolean string must be set to "Yes" if the user should have Remote Console privileges. If this parameter is used, the Boolean string value must never be left blank. Leaving out this privilege will deny the user access to any Remote Console functionality.

RESET\_SERVER\_PRIV is a Boolean parameter that gives the user permission to remotely reset the server or power it down. This parameter is optional, and the Boolean string must be set to "Yes" if the user is allowed to modify the server power. If this parameter is used, the Boolean string value must never be left blank. Leaving out this parameter denies the user server reset privileges.

VIRTUAL\_MEDIA\_PRIV is a Boolean parameter that gives the user permission to access the virtual floppy functionality. This parameter is optional, and the Boolean string must be set to "Yes" if the user should have virtual floppy privileges. If this parameter is used, the Boolean string value must never be left blank. Leaving out this parameter denies the user virtual floppy privileges.



CONFIG\_ILO\_PRIV is a Boolean parameter that allows the user to configure iLO settings. This privilege includes network settings, global settings, Insight Manager settings, and SNMP settings. This parameter is optional, and the Boolean string must be set to "Yes" if the user should be allowed to configure iLO. If this parameter is used, the Boolean string value must never be blank.

**NOTE:** The following parameters are not applicable to a user's privileges in iLO firmware versions 1.40 and higher. The parameters will parse correctly, but user privileges will not be affected.

VIEW\_LOGS\_PRIV is a Boolean parameter that gives the user permission to view the iLO system logs. This parameter is optional, and the Boolean string must be set to "Yes" if the user should be allowed to view logs. If this parameter is used, the Boolean string value must never be blank.

CLEAR\_LOGS\_PRIV is a Boolean parameter that gives the user permission to clear the event log. This parameter is optional, and the Boolean string must be set to "Yes" if the user should be allowed to clear the iLO event log. If this parameter is used, the Boolean string value must never be blank.

EMS\_PRIV is a Boolean parameter that gives the user permission to use the Windows® Server 2003 EMS service. This parameter is optional, and the Boolean string must be set to "Yes" if the user should be allowed to use EMS services. If this parameter is used, the Boolean string value must never be blank.

UPDATE\_ILO\_PRIV is a Boolean parameter that allows the user to copy a new firmware image into the iLO system ROM. This parameter is optional, and the Boolean string must be set to "Yes" if the user should be allowed to configure iLO. If this parameter is used, the Boolean string value must never be blank.

CONFIG\_RACK\_PRIV is a Boolean parameter that gives the user permission to configure and manage the server rack resources. This parameter is applicable to ProLiant BL p-Class servers only. This parameter is optional, and the Boolean string must be set to "Yes" if the user should be allowed to manage or configure rack resources. If this parameter is used, the Boolean string value must never be blank.

DIAG\_PRIV is a Boolean parameter that gives the user permission to view diagnostic information about iLO. This parameter is optional, and the Boolean string must be set to "Yes" if the user should have diagnostic privileges. If this parameter is used, the Boolean string value must never be blank.

## ADD\_USER Runtime Errors

The possible ADD\_USER error messages include:

- Login name is too long. Maximum length is 39 characters.
- Password is too short. Minimum length is 8 characters.
- Password is too long. Maximum length is 39 characters.
- User table is full. No room for new user.
- Cannot add user. The user name already exists.
- User information is open for read-only access. Write access is required for this operation.
- User name cannot be blank.
- User login ID cannot be blank.
- Password must not be blank.
- Boolean value not specified.
- User does not have correct privilege for action.
- Logged-in user does not have required privilege for this command.

## DELETE\_USER

The DELETE\_USER command is used to remove an existing local user's information. Before this command is used, the USER\_INFO command must have been issued with the mode set to "write." The user must have administrative privilege to delete other user accounts.

Example:

```
<RIBCL VERSION="2.0">
  <LOGIN USER_LOGIN="adminname"
    PASSWORD="password">
    <USER_INFO MODE="write">
      <DELETE_USER USER_LOGIN="username"/>
    </USER_INFO>
  </LOGIN>
```

---

```
</RIBCL>
```

## DELETE\_USER Parameter

USER\_LOGIN is the login name of the user that you want to delete. The USER\_LOGIN parameter has a maximum length of 39 characters, can be an ASCII string containing any combination of printable characters, and is case sensitive. The USER\_LOGIN parameter must never be blank.

## DELETE\_USER Runtime Errors

The possible DELETE\_USER errors include:

- User information is open for read-only access. Write access is required for this operation.
- Cannot delete user information for currently logged in user.
- User login name was not found.
- User login name must not be blank.
- User does not have correct privilege for action.
- Logged in user does not have required privileges for this command.

## GET\_USER

The GET\_USER command returns the local user's information, excluding the password. The user must have login privilege to execute this command. If the user does not have administrative privileges, only the logged user's information can be retrieved.

Example:

```
<RIBCL VERSION="2.0">
  <LOGIN USER_LOGIN="adminname" PASSWORD="password">
    <USER_INFO MODE="read">
      <GET_USER USER_LOGIN="username"/>
    </USER_INFO>
  </LOGIN>
</RIBCL>
```

## GET\_USER Parameter

USER\_LOGIN is the name that the user types in to log in to iLO. This parameter is case sensitive, can be any valid string, and has a maximum length of 39 characters. The string must never be blank.

The user must have the Administer User Accounts privilege to retrieve other user accounts. A user without the administrative privilege can only view their own account information.

## GET\_USER Runtime Errors

The possible GET\_USER error messages include:

- User login ID cannot be blank.
- User login name was not found.
- Logged-in user does not have required privilege for this command.

## GET\_USER Return Messages

A possible GET\_USER return message includes:

```
<RESPONSE
  STATUS="0x0000"
  MSG="No Errors"
/>
<GET_USER
  USER_NAME="Admin User"
  USER_LOGIN= "username"
  ADMIN_PRIV="N"
  REMOTE_CONS_PRIV="Y"
  RESET_SERVER_PRIV="N"
  VIRTUAL_MEDIA_PRIV="N"
  CONFIG_ILO_PRIV value ="No"
/>
```

## MOD\_USER

The MOD\_USER command is used to modify an existing local user's information. You are not required to enter any of the fields except for the first one, which specifies which user to modify. If any parameter does not need to be modified, you should omit it. MOD\_USER must be displayed within a USER\_INFO parameter, and USER\_INFO must be in write mode. The user login name used to gain access cannot be modified.

To modify user names, user passwords, or user rights, the user must be logged in with the administrative privilege. A user without administrative privilege can only modify their account password.

Example:

```
<RIBCL VERSION="2.0">
  <LOGIN USER_LOGIN="adminname" PASSWORD="password">
    <USER_INFO MODE="write">
      <MOD_USER USER_LOGIN="loginname">
        <USER_NAME value="username"/>
        <PASSWORD value="password"/>
        <ADMIN_PRIV value="No"/>
        <REMOTE_CONS_PRIV value="Yes"/>
        <RESET_SERVER_PRIV value="No"/>
        <CONFIG_ILO_PRIV value="Yes"/>
        <VIRTUAL_MEDIA_PRIV value="No"/>
      </MOD_USER>
    </USER_INFO>
  </LOGIN>
</RIBCL>
```

## MOD\_USER Parameters

USER\_LOGIN is the name that the user types in to log in to iLO. This parameter is case sensitive, can be any valid string, and has a maximum length of 39 characters. The string must never be blank.

**NOTE:** If the following parameters are not specified, then the parameter value for the specified user is not changed.

USER\_NAME is the actual name of the user to be added. This parameter is case sensitive, can be any valid string, and has a maximum length of 39 characters. This string is used for display only and must never be blank.

PASSWORD is the password that will be associated with the user. This parameter has a minimum length of 0 characters, a maximum length of 39 characters, depending on the minimum password length set on the Global Settings screen. PASSWORD is an ASCII string that may contain any combination of printable characters. The PASSWORD parameter cannot contain both single and double quote characters. This parameter is case sensitive.

ADMIN\_PRIV is a Boolean parameter that allows the user to administer user accounts. The user can modify their account settings, modify other user account settings, add users, and delete users. Leaving out this parameter prevents the user from adding, deleting, or configuring accounts.

REMOTE\_CONS\_PRIV is a Boolean parameter that gives permission for the user to access the Remote Console functionality. This parameter is optional, and the Boolean string must be set to "Yes" if the user should have Remote Console privileges. If this parameter is used, the Boolean string value must never be left blank. Leaving out this privilege will deny the user access to any Remote Console functionality.

RESET\_SERVER\_PRIV is a Boolean parameter that gives the user permission to remotely reset the server or power it down. This parameter is optional, and the Boolean string must be set to "Yes" if the user is allowed to modify the server power. If this parameter is used, the Boolean string value must never be left blank. Leaving out this parameter denies the user server reset privileges.

CONFIG\_ILO\_PRIV is a Boolean parameter that allows the user to configure iLO settings. This privilege includes network settings, global settings, Insight Manager settings, and SNMP settings. This parameter is optional, and the Boolean string must be set to "Yes" if the user should be allowed to configure iLO. If this parameter is used, the Boolean string value must never be blank.

VIRTUAL\_MEDIA\_PRIV is a Boolean parameter that gives the user permission to access the virtual floppy functionality. This parameter is optional, and the Boolean string must be set to "Yes" if the user should have virtual floppy privileges. If this parameter is used, the Boolean string value must never be left blank. Leaving out this parameter denies the user virtual floppy privileges.

## MOD\_USER Runtime Errors

The possible MOD\_USER error messages include:

- Login name is too long. Maximum length is 39 characters.
- Password is too short. Minimum length is 8 characters.
- Password is too long. Maximum length is 39 characters.
- User information is open for read-only access. Write access is required for this operation.
- User login ID cannot be blank.
- Cannot modify user information for currently logged user.
- This user is not logged in.
- User does not have correct privilege for action.
- Logged-in user does not have required privilege for this command.

## GET\_ALL\_USERS

The GET\_ALL\_USERS command requests a list of all of the valid user names that are currently in the local user database. The user database must have been successfully opened with the USER\_INFO command and must have been opened in read or write mode for this command to work. The user must have administrative privilege to execute this command.

Example:

```
<RIBCL VERSION="2.0">  
  <LOGIN USER_LOGIN="adminname" PASSWORD="password">  
  <USER_INFO MODE="read">  
  <GET_ALL_USERS />
```

```
    </USER_INFO>
  </LOGIN>
</RIBCL>
```

## **GET\_ALL\_USERS Runtime Error**

Logged in user does not have required privileges for this command.

## **GET\_ALL\_USERS Return Messages**

A possible GET\_ALL\_USERS return message is:

```
<RESPONSE
  STATUS="0x0000"
  MESSAGE='No Error'
/>
  USER_LOGIN="username"
  USER_LOGIN="user2"
  USER_LOGIN="user3"
  USER_LOGIN="user4"
  USER_LOGIN="user5"
  USER_LOGIN="user6"
  USER_LOGIN="user7"
  USER_LOGIN="user8"
  USER_LOGIN="user9"
  USER_LOGIN="user10"
  USER_LOGIN="user11"
  USER_LOGIN="user12"
/>
```

A possible unsuccessful request is:

```
<RESPONSE
  STATUS = "0x0001"
  MSG = "Error Message"/>
```



## GET\_ALL\_USER\_INFO

The GET\_ALL\_USER\_INFO command requests the return of the current local user database. This command returns detailed information on each user and not just the user login name. The user database must have been successfully opened with the USERS\_INFO command. The USER\_INFO command can be opened in either read or write mode. GET\_ALL\_USER\_INFO requires the user to log in with administrative privilege.

Example:

```
<RIBCL VERSION="2.0">
  <LOGIN USER_LOGIN="adminname" PASSWORD="password">
    <USER_INFO MODE="read">
      <GET_ALL_USER_INFO />
    </USER_INFO>
  </LOGIN>
</RIBCL>
```

## GET\_ALL\_USER\_INFO Parameters

There are no parameters for this command.

## GET\_ALL\_USER\_INFO Runtime Errors

A possible GET\_ALL\_USER\_INFO error is: Logged in user does not have required privilege for this command.

## GET\_ALL\_USER\_INFO

A possible GET\_ALL\_USER\_INFO return message is:

```
<RESPONSE
  STATUS="0x0000"
  MSG="No Errors"
/>
<GET_USER
  USER_NAME="Admin"
  USER_LOGIN="Admin"
  ADMIN_PRIV="Y"
```

```
CONFIG_RILO_PRIV="Y"  
LOGIN_PRIV="Y"  
REMOTE_CONS_PRIV="Y"  
RESET_SERVER_PRIV="Y"  
VIRTUAL_MEDIA_PRIV="Y"  
/> .....
```

The same information will be repeated for all the users.

A possible unsuccessful request is:

```
<RESPONSE  
  STATUS = "0x0001"  
MSG = "Error Message"/>
```

## RIB\_INFO

The RIB\_INFO command tells the firmware that the configuration of the iLO is about to be changed.

Example:

```
<RIB_INFO MODE="write">  
..... RIB_INFO commands .....  
</RIB_INFO>
```

## RIB\_INFO Parameter

MODE is a specific string parameter with a maximum length of 10 characters that specifies what you intend to do with the user information. Valid arguments are "read" and "write."

Write mode enables both reading and writing, and other users will be unable to open the iLO information. Read mode prevents the user from changing any iLO data. Read mode is assumed if the mode attribute is left out.

## RIB\_INFO Runtime Errors

There are no RIB\_INFO errors.

## RESET\_RIB

This command allows the user to reset the iLO. RESET\_RIB must display inside a RIB\_INFO block in write mode. The user must be logged in with configure iLO privilege to execute this command.

Example:

```
<RIBCL VERSION="2.0">
  <LOGIN USER_LOGIN="Admin" PASSWORD="Password">
    <RIB_INFO MODE = "write">
      <RESET_RIB/>
    </RIB_INFO>
  </LOGIN>
</RIBCL>
```

### RESET\_RIB Parameters

There are no parameters for this command.

### RESET\_RIB Runtime Errors

There are no errors for this command.

## GET\_NETWORK\_SETTINGS

The GET\_NETWORK\_SETTINGS command allows the user to retrieve the network settings. GET\_NETWORK\_SETTINGS must display inside a RIB\_INFO block. The user must have login privilege to execute this command.

Example:

```
<RIBCL VERSION="2.0">
  <LOGIN USER_LOGIN="adminname" PASSWORD="password">
    <RIB_INFO MODE="read">
      <GET_NETWORK_SETTINGS/>
    </RIB_INFO>
  </LOGIN>
</RIBCL>
```

## GET\_NETWORK\_SETTINGS Parameters

There are no parameters for this command.

## GET\_NETWORK\_SETTINGS Runtime Errors

There are no errors for this command.

## GET\_NETWORK\_SETTINGS Return Messages

A possible GET\_NETWORK\_SETTINGS return message is:

```
<GET_NETWORK_SETTINGS
  SPEED_AUTOSELECT="YES"
  NIC_SPEED="100"
  FULL_DUPLEX="NO"
  DHCP_ENABLE="YES"
  DHCP_GATEWAY="YES"
  DHCP_DNS_SERVER="YES"
  DHCP_STATIC_ROUTE="YES"
  DHCP_WINS_SERVER="YES"
  REG_WINS_SERVER="YES"
  IP_ADDRESS="111.111.111.111"
  SUBNET_MASK="255.255.255.0"
  GATEWAY_IP_ADDRESS="111.111.111.1"
  DNS_NAME="test"
  DOMAIN_NAME="test.com"
  PRIM_DNS_SERVER="111.111.111.242"
  SEC_DNS_SERVER="111.111.111.242"
  TER_DNS_SERVER="111.111.111.242"
  PRIM_WINS_SERVER="111.111.111.246"
  SEC_WINS_SERVER="111.111.111.247"
  STATIC_ROUTE_1 DEST="0.0.0.0" GATEWAY="0.0.0.0"
  STATIC_ROUTE_2 DEST="0.0.0.0" GATEWAY="0.0.0.0"
  STATIC_ROUTE_3 DEST="0.0.0.0" GATEWAY="0.0.0.0"
  WEB_AGENT_IP_ADDRESS=""
/>
```

A possible unsuccessful request is:

```
<RESPONSE
  STATUS = "0x0001"
```

```
MSG = "Error Message"/>
```

## MOD\_NETWORK\_SETTINGS

MOD\_NETWORK\_SETTINGS is used to modify certain network settings. This command is only valid inside a RIB\_INFO block. The logged-in user must have the Configure iLO Settings privilege, and the mode of the containing RIB\_INFO block must be "write." All of these elements are optional, and may be left out. If an element is left out, then the current setting is preserved. The iLO Management Processor will reboot to apply the changes after the MOD\_NETWORK\_SETTINGS command is closed.

When modifying network settings, the user should be cognizant of the network commands provided to the management processor. In some cases, the management processor will ignore commands and no error will be returned. For example, when a script includes the command to enable DHCP and a command to modify the IP address, the IP address will be ignored. Changing the network settings to values that are not correct for the network may cause a loss of connectivity to the iLO. The iLO scripting firmware does not attempt to determine if the settings are appropriate for the network configuration.

If connectivity is lost to the iLO, you must use the RBSU to reconfigure the network settings to values that are compatible with the network. For more information, refer to the "iLO RBSU (on page 14)" section.

Example:

```
<RIBCL VERSION="2.0">
  <LOGIN USER_LOGIN="adminname" PASSWORD="password">
  <RIB_INFO MODE="write">
  <MOD_NETWORK_SETTINGS>
    <ENABLE_NIC value="Yes"/>
    <SPEED_AUTOSELECT value="No"/>
    <NIC_SPEED value="100"/>
    <FULL_DUPLEX value="Yes"/>
    <DHCP_ENABLE value="Yes"/>
    <IP_ADDRESS value="192.168.132.25"/>
    <SUBNET_MASK value="255.255.0.0"/>
    <GATEWAY_IP_ADDRESS value="192.168.132.2"/>
    <DNS_NAME value="demorib"/>
    <DOMAIN_NAME value="internal.net"/>
    <DHCP_GATEWAY value="No"/>
```

```
<DHCP_DNS_SERVER value="No"/>
<DHCP_WINS_SERVER value="No"/>
<DHCP_STATIC_ROUTE value="No"/>
<REG_WINS_SERVER value="No"/>
<REG_DDNS_SERVER value="No"/>
<PING_GATEWAY value="Yes"/>
<PRIM_DNS_SERVER value="192.168.12.14"/>
<SEC_DNS_SERVER value="192.168.12.15"/>
<TER_DNS_SERVER value="192.168.12.16"/>
<PRIM_WINS_SERVER value="192.168.145.1"/>
<SEC_WINS_SERVER value="192.168.145.2"/>
<STATIC_ROUTE_1 DEST="192.168.129.144"
GATEWAY="192.168.129.1"/>
<STATIC_ROUTE_2 DEST="192.168.129.145"
GATEWAY="192.168.129.2"/>
<STATIC_ROUTE_3 DEST="192.168.129.146"
GATEWAY="192.168.129.3"/>
</MOD_NETWORK_SETTINGS>
</RIB_INFO>
</LOGIN>
</RIBCL>
```

## MOD\_NETWORK\_SETTINGS Parameters

**SPEED\_AUTOSELECT** is used to automatically select the transceiver speed. The possible values are "Yes" or "No." It is case insensitive.

**FULL\_DUPLEX** is used to decide if the iLO is to support full-duplex or half-duplex mode. It is only applicable if **SPEED\_AUTOSELECT** was set to "No." The possible values are "Yes" or "No." It is case insensitive.

**NIC\_SPEED** is used to set the transceiver speed if **SPEED\_AUTOSELECT** was set to "No." The possible values are "10" or "100." Any other values will result in a syntax error.

**DHCP\_ENABLE** is used to enable DHCP. The possible values are "Yes" or "No." It is case insensitive.

**IP\_ADDRESS** is used to select the IP address for the iLO if DHCP is not enabled. If an empty string is entered, the current value is deleted.

SUBNET\_MASK is used to select the subnet mask for the iLO if DHCP is not enabled. If an empty string is entered, the current value is deleted.

GATEWAY\_IP\_ADDRESS is used to select the default gateway IP address for the iLO if DHCP is not enabled. If an empty string is entered, the current value is deleted.

DNS\_NAME is used to specify the DNS name for the iLO. If an empty string is entered, the current value is deleted.

DOMAIN\_NAME is used to specify the domain name for the network where the iLO resides. If an empty string is entered, the current value is deleted.

DHCP\_GATEWAY specifies if the DHCP-assigned gateway address is to be used. The possible values are "Yes" or "No." It is case sensitive. This selection is only valid if DHCP is enabled.

DHCP\_DNS\_SERVER specifies if the DHCP-assigned DNS server is to be used. The possible values are "Yes" or "No." It is case sensitive. This selection is only valid if DHCP is enabled.

DHCP\_WINS\_SERVER specifies if the DHCP-assigned WINS server is to be used. The possible values are "Yes" or "No." It is case sensitive. This selection is only valid if DHCP is enabled.

DHCP\_STATIC\_ROUTE specifies if the DHCP-assigned static routes are to be used. The possible values are "Yes" or "No." It is case sensitive. This selection is only valid if DHCP is enabled.

REG\_WINS\_SERVER specifies if the iLO needs to register with the WINS server. The possible values are "Yes" or "No." It is case sensitive. This selection is only valid if DHCP is enabled.

PRIM\_DNS\_SERVER specifies the IP address of the primary DNS server. This parameter is only relevant if the DHCP-assigned DNS server address feature is disabled. If an empty string is entered, the current value is deleted.

SEC\_DNS\_SERVER specifies the IP address of the secondary DNS server. This parameter is only relevant if the DHCP-assigned DNS server address feature is disabled. If an empty string is entered, the current value is deleted.

TER\_DNS\_SERVER specifies the IP address of the tertiary DNS server. This parameter is only relevant if the DHCP-assigned DNS server address feature is disabled. If an empty string is entered, the current value is deleted.

PRIM\_WINS\_SERVER specifies the IP address of the primary WINS server. This parameter is only relevant if the DHCP-assigned WINS server address feature is disabled. If an empty string is entered, the current value is deleted.

SEC\_WINS\_SERVER specifies the IP address of the secondary WINS server. This parameter is only relevant if the DHCP-assigned WINS server address feature is disabled. If an empty string is entered, the current value is deleted.

STATIC\_ROUTE\_1, STATIC\_ROUTE\_2, and STATIC\_ROUTE\_3 are used to specify the destination and gateway IP addresses of the static routes. The following two parameters are used within the static route commands. If an empty string is entered, the current value is deleted.

- DEST specifies the destination IP addresses of the static route. This parameter is only relevant if the DHCP-assigned static route feature is disabled. If an empty string is entered, the current value is deleted.
- GATEWAY specifies the gateway IP addresses of the static route. This parameter is only relevant if the DHCP-assigned static route feature is disabled. If an empty string is entered, the current value is deleted.

WEB\_AGENT\_IP\_ADDRESS specifies the address for the Web-enabled agents. If an empty string is entered, the current value is deleted.

**NOTE:** The iLO is rebooted to apply the changes after MOD\_NETWORK\_SETTINGS has been closed.

## MOD\_NETWORK\_SETTINGS Runtime Errors

The possible MOD\_NETWORK\_SETTINGS error messages include:

- RIB information is open for read-only access. Write access is required for this operation.
- User does not have correct privilege for action.
- Logged-in user does not have required privilege for this command.



## MOD\_DIAGPORT\_SETTINGS

This command is used to modify certain network settings on the iLO Diagnostic Port. This command is only valid inside a RACK\_INFO block on a ProLiant BL p-Class series server. The logged-in user must have the Configure iLO privilege and the mode of the containing RACK\_INFO block must be "write."

DP\_IP\_ADDRESS and DP\_SUBNET\_MASK should not be left empty. For both parameters, if an empty string is entered, the current address is deleted.

Example:

```
<RIBCL VERSION="2.0">
  <LOGIN USER_LOGIN="username" PASSWORD="password">
    <RACK_INFO MODE="write">
      <MOD_DIAGPORT_SETTINGS>
        <DP_SPEED_AUTOSELECT value="No"/>
        <DP_NIC_SPEED value="100"/>
        <DP_FULL_DUPLEX value="Yes"/>
        <DP_IP_ADDRESS value="192.168.142.56"/>
        <DP_SUBNET_MASK value="255.255.0.0"/>
      </MOD_DIAGPORT_SETTINGS>
    </RACK_INFO>
  </LOGIN>
</RIBCL>
```

### MOD\_DIAGPORT\_SETTINGS Parameters

DP\_SPEED\_AUTOSELECT is used to automatically select the transceiver speed. The possible values are "Yes" or "No." It is case insensitive.

DP\_NIC\_SPEED is used to set the transceiver speed if DP\_SPEED\_AUTOSELECT was set to "No." The possible values are 10 or 100. Any other value results in a syntax error.

DP\_FULL\_DUPLEX is used to decide if the iLO diagnostic port is to support full-duplex or half-duplex mode. It is only applicable if DP\_SPEED\_AUTOSELECT was set to "No." The possible values are "Yes" or "No." It is case insensitive.

DP\_IP\_ADDRESS is used to select the IP address for the iLO Diagnostic Port. If an empty string is entered, the current address is unchanged. The expected format is XXX.XXX.XXX.XXX.

DP\_SUBNET\_MASK is used to select the subnet mask for the iLO Diagnostic Port. If an empty string is entered, the current address is unchanged. The expected format is XXX.XXX.XXX.XXX.

**NOTE:** When MOD\_DIAGPORT\_SETTINGS has been closed, iLO will reboot to apply the changes. Integrated Lights-Out will not reboot if there are any runtime errors.

## MOD\_DIAGPORT\_SETTINGS Runtime Errors

Possible MOD\_DIAGPORT\_SETTINGS error messages include:

- iLO information is open for read-only access. Write access is required for this operation.
- Logged-in user does not have required privilege for this command.

## DIR\_INFO

The DIR\_INFO command is used to display information on the server. Only commands that are DIR\_INFO type commands are valid inside the DIR\_INFO block.

```
<DIR_INFO MODE="read">
</DIR_INFO>
```

### DIR\_INFO Parameter

MODE is a specific string parameter with a maximum length of 10 characters that specifies what you intend to do with the user information. Valid arguments are "read" and "write."

### DIR\_INFO Runtime Errors

- Mode parameter must not be blank.

- User does not have correct privilege for action.

## GET\_DIR\_CONFIG

The GET\_DIR\_CONFIG command gets the directory configuration of the iLO. This command must be contained within a DIR\_INFO block. All parameters are optional. The user must be logged in with login privilege to execute this command.

Example:

```
<RIBCL VERSION="2.0">
  <LOGIN USER_LOGIN="adminname" PASSWORD="password">
    <DIR_INFO MODE="read">
      <GET_DIR_CONFIG/>
    </DIR_INFO>
  </LOGIN>
</RIBCL>
```

### GET\_DIR\_CONFIG Parameters

There are no parameters for this command.

### GET\_DIR\_CONFIG Runtime Errors

There are no errors for this command.

### GET\_DIR\_CONFIG Return Messages

A possible GET\_DIR\_CONFIG return message is:

```
<RESPONSE
STATUS="0x0000"
MSG = 'No Error'
/>
<GET_DIR_CONFIG
DIR_AUTHENTICATION_ENABLED = "YES"
DIR_LOCAL_USER_ACCT = "YES"
DIR_SERVER_ADDRESS = "server1.hprib.labs"
DIR_SERVER_PORT = "636"
```

```
DIR_OBJECT_DN = "CN=SERVER1_RIB, OU=RIB, DC=HPRIB,  
DC=LABS"  
DIR_USER_CONTEXT1 = "CN=Users0, DC=HPRIB0, DC=LABS"  
DIR_USER_CONTEXT2 = "CN=Users1, DC=HPRIB1, DC=LABS"  
DIR_USER_CONTEXT3 = ""  
</>
```

A possible unsuccessful request is:

```
<RESPONSE  
  STATUS = "0x0001"  
  MSG = "Error Message"/>
```

## MOD\_DIR\_CONFIG

The MOD\_DIR\_CONFIG command will modify certain directory settings. Directories are used for user authentication. This command is only valid inside a DIR\_INFO block. The logged-in user must have the configure iLO privilege and the mode of the containing DIR\_INFO block must be "write." All of these parameters are optional and may be left out. If a parameter is left out, then the current setting is preserved. If any value is set to an empty string, then the previous value is erased.

Example:

```
<RIBCL VERSION="2.0">  
  <LOGIN USER_LOGIN="adminname" PASSWORD="password">  
    <DIR_INFO MODE="write">  
      <MOD_DIR_CONFIG>  
        <DIR_AUTHENTICATION_ENABLED value="Yes"/>  
        <DIR_LOCAL_USER_ACCT value="Yes"/>  
        <DIR_SERVER_ADDRESS value="16.141.100.44"/>  
        <DIR_SERVER_PORT value="636"/>  
        <DIR_OBJECT_DN value="CN=server1_rib, OU=RIB,  
        DC=HPRIB, DC=LABS"/>  
        <DIR_OBJECT_PASSWORD value="password"/>  
        <DIR_USER_CONTEXT_1 value="CN=Users, DC=HPRIB,  
        DC=LABS"/>  
      </MOD_DIR_CONFIG>  
    </DIR_INFO>  
  </LOGIN>  
</RIBCL>
```

## MOD\_DIR\_CONFIG Parameters

DIR\_AUTHENTICATION\_ENABLED enables or disables directory authentication. The possible values are "Yes" and "No."

DIR\_LOCAL\_USER\_ACCT enables or disables local user accounts.

DIR\_SERVER\_ADDRESS indicates the location of the directory server. The directory server location is specified as an IP address or DNS name.

DIR\_SERVER\_PORT indicates the port number used to connect to the directory server. This value is obtained from the directory administrator. The secured LDAP port is 636, but the directory server can be configured for a different port number.

DIR\_OBJECT\_DN specifies the unique name of the iLO board in the directory server. This value is obtained from the directory administrator. Distinguished names are limited to 256 characters.

DIR\_OBJECT\_PASSWORD specifies the password associated with the iLO object in the directory server. Passwords are limited to 39 characters.

DIR\_USER\_CONTEXT\_1, DIR\_USER\_CONTEXT\_2, and DIR\_USER\_CONTEXT\_3 specify searchable contexts used to locate the user when the user is trying to authenticate using directories. If the user could not be located using the first path, then the parameters specified in the second and third paths are used. The values for these parameters are obtained from the directory administrator. Directory User Contexts are limited to 128 characters each.

## MOD\_DIR\_CONFIG Runtime Errors

The possible MOD\_DIR\_CONFIG error messages include:

- Directory information is open for read-only access. Write access is required for this operation.
- Logged-in user does not have required privilege for this command.

## GET\_GLOBAL\_SETTINGS

The GET\_GLOBAL\_SETTINGS command allows the user to retrieve the global settings. GET\_GLOBAL\_SETTINGS must be contained inside a RIB\_INFO block. The user must be logged in with login privilege for this command. The information returned by this command is the information that can be changed by the MOD\_GLOBAL\_SETTINGS command.

### GET\_GLOBAL\_SETTINGS Parameters

There are no parameters for this command.

### GET\_GLOBAL\_SETTINGS Runtime Errors

There are no errors for this command.

### GET\_GLOBAL\_SETTINGS Return Messages

A possible GET\_GLOBAL\_SETTINGS return message is:

```
<GET_GLOBAL_SETTINGS
  SESSION_TIMEOUT="120"
  F8_PROMPT_ENABLED="YES"
  REMOTE_CONSOLE_PORT_STATUS ="ENABLED"
  HTTPS_PORT ="443"
  HTTP_PORT ="80"
  REMOTE_CONSOLE_PORT ="23"
  VIRTUAL_MEDIA_PORT = "17988"
  SNMP_ADDRESS_1 =" "
  SNMP_ADDRESS_2 =" "
  SNMP_ADDRESS_3 =" "
  OS_TRAPS ="NO"
  RIB_TRAPS ="NO"
  CIM_SECURITY_MASK ="MEDIUM"
/>
```

The following is an example of an unsuccessful request:

```
<RESPONSE
  STATUS = "0x0001"
```

```
MSG = "Error Message"/>
```

## MOD\_GLOBAL\_SETTINGS

This command is used to modify certain global settings. The MOD\_GLOBAL\_SETTINGS command must appear within a RIB\_INFO element and RIB\_INFO must be in write mode. The logged-in user must have the Configure iLO privilege. All of these elements are optional, and may be left out. If an element is left out, then the current setting is preserved. This command modifies certain global settings.

Example:

```
<RIBCL VERSION="2.0">
  <LOGIN USER_LOGIN="adminname" PASSWORD="password">
    <RIB_INFO MODE="write">
      <MOD_GLOBAL_SETTINGS>
        <SESSION_TIMEOUT value="60"/>
        <ILO_FUNCT_ENABLED value="Yes"/>
        <F8_PROMPT_ENABLED value="Yes"/>
        <HTTPS_PORT value="443"/>
        <HTTP_PORT value="80"/>
        <REMOTE_CONSOLE_PORT value="23"/>
        <VIRTUAL_MEDIA_PORT value="17988"/>
      </MOD_GLOBAL_SETTINGS>
    </RIB_INFO>
  </LOGIN>
</RIBCL>
```

## MOD\_GLOBAL\_SETTINGS Parameters

SESSION\_TIMEOUT determines the maximum session timeout value in minutes. The accepted values are from 15, 30, 60 and 120. If a value greater than 120 is specified, the SESSION\_TIMEOUT returns an error.

ILO\_FUNCT\_ENABLED determines if the Lights-Out functionality is enabled or disabled for iLO. The possible values are "Yes" or "No." It is case insensitive.

F8\_PROMPT\_ENABLED determines if the F8 prompt for ROM-based configuration is displayed during POST. The possible values are "Yes" or "No."

HTTPS\_PORT specifies the HTTPS (SSL) port number for the <LOM\_short-name>. If this value is changed, the iLO must be reset.

HTTP\_PORT specifies the HTTP port number for the iLO. If this value is changed, the iLO must be reset.

REMOTE\_CONSOLE\_PORT specifies the Remote Console port for the iLO. The iLO must be reset if this value is changed.

REMOTE\_CONSOLE\_ENCRYPTION determines if Remote Console Data Encryption is enabled or disabled. The possible values are "Yes" and "No."

VIRTUAL\_MEDIA\_PORT specifies the port used for virtual media on iLO. iLO must be reset if this value is changed.

**NOTE:** iLO will reboot to apply the port changes. iLO will not reboot if there are any runtime errors.

MIN\_PASSWORD command specifies how many characters are required in all user passwords. The value can be from 0 to 39 characters.

## MOD\_GLOBAL\_SETTINGS Runtime Errors

The possible MOD\_GLOBAL\_SETTINGS error messages include:

- RIB information is open for read-only access. Write access is required for this operation.
- Logged-in user does not have required privilege for this command.
- Maximum password length value exceeded.

## MOD\_SNMP\_IM\_SETTINGS

This command enables the user to modify certain SNMP and Insight Manager settings. The MOD\_SNMP\_IM\_SETTINGS must appear within a RIB\_INFO element and RIB\_INFO must be in write mode. The logged-in user must have the Configure iLO privilege. All of these elements are optional, and may be left out. If an element is left out, then the current setting is preserved.

Example:



```

<RIBCL VERSION="2.0">
  <LOGIN USER_LOGIN="adminname" PASSWORD="password">
    <RIB_INFO MODE="write">
      <MOD_SNMP_IM_SETTINGS>
        <WEB_AGENT_IP_ADDRESS value="192.168.125.120"/>
        <SNMP_ADDRESS_1 value="192.168.125.121"/>
        <SNMP_ADDRESS_2 value="192.168.125.122"/>
        <SNMP_ADDRESS_3 value="192.168.125.123"/>
        <OS_TRAPS value="Yes"/>
        <RIB_TRAPS value="No"/>
        <CIM_SECURITY_MASK value="3"/>
      </MOD_SNMP_IM_SETTINGS>
    </RIB_INFO>
  </LOGIN>
</RIBCL>

```

## MOD\_SNMP\_IM\_SETTINGS Parameters

WEB\_AGENT\_IP\_ADDRESS is the address for the Web-enabled agents. The value for this element has a maximum length of 50 characters. It can be any valid IP address or DNS name. If an empty string is entered, the current value is deleted.

SNMP\_ADDRESS\_1, SNMP\_ADDRESS\_2, and SNMP\_ADDRESS\_3 are the addresses that receive traps sent to the user. Each of these parameters can be any valid IP address or DNS name and has a maximum value of 50 characters.

OS\_TRAPS indicates that the user should receive SNMP traps that are generated by the operating system. The possible values are "Yes" and "No." If the value is not set, then the default "No" is assumed, and traps are not sent.

RIB\_TRAPS indicates that the user should receive SNMP traps that are generated by the RIB. The possible values are "Yes" and "No." If the value is not set, then the default "No" is assumed, and traps are not sent.

CIM\_SECURITY\_MASK accepts an integer between 0 and 4. The possible values are:

- **0**—No change
- **1**—None (No data is returned to Insight Manager 7.)

- **2**—Low (Name and status data are returned. Associations are present if SNMP pass-through is supported. If not, the server and management processor are separate entities in the device list.)
- **3**—Medium (iLO and server associations are present but the summary page contains less detail than at high security.)
- **4**—High (Associations are present and all data is present on the summary page.)

Each value indicates the level of data returned to an Insight Manager 7 request.

## MOD\_SNMP\_IM\_SETTINGS Runtime Errors

- User does not have correct privilege for action.
- RIB information is open for read-only access. Write access is required for this operation.

## CLEAR\_EVENTLOG

The CLEAR\_EVENTLOG command clears the iLO Event Log. The CLEAR\_EVENTLOG command must be displayed within a RIB\_INFO block, and RIB\_INFO must be in write mode. To clear the event log, the user must be logged in with the configure iLO privilege.

Example:

```
<RIBCL VERSION="2.0">
  <LOGIN USER_LOGIN="adminname" PASSWORD="password">
    <RIB_INFO MODE="write">
      <CLEAR_EVENTLOG/>
    </RIB_INFO>
  </LOGIN>
</RIBCL>
```

## CLEAR\_EVENTLOG Parameters

There are no parameters for this command.

## CLEAR\_EVENTLOG Runtime Errors

The possible CLEAR\_EVENTLOG error messages are:

- RIB information is open for read-only access. Write access is required for this operation.
- User does not have correct privilege for action.
- Logged-in user does not have required privilege for this command.

## UPDATE\_RIB\_FIRMWARE

The UPDATE\_RIB\_FIRMWARE command copies the firmware upgrade file to the iLO, starts the upgrade process and reboots the board after the image has been flashed successfully. The UPDATE\_RIB\_FIRMWARE command must be displayed within a RIB\_INFO block, and RIB\_INFO must be in write mode. The iLO is reset after the firmware upgrade is complete. To update the firmware, the user must be logged in with the configure iLO privilege.

Example:

```
<RIBCL VERSION="2.0">
  <LOGIN USER_LOGIN="adminname" PASSWORD="password">
    <RIB_INFO MODE="write">
      <UPDATE_RIB_FIRMWARE IMAGE_LOCATION="C:\ILO140.BIN"/>
    </RIB_INFO>
  </LOGIN>
</RIBCL>
```

## UPDATE\_RIB\_FIRMWARE Parameters

IMAGE\_LOCATION takes the full path file name of the firmware upgrade file.

## UPDATE\_RIB\_FIRMWARE Runtime Errors

The possible UPDATE\_RIB\_FIRMWARE error messages include:

- RIB information is open for read-only access. Write access is required for this operation.

- Unable to open the firmware image update file.
- Unable to read the firmware image update file.
- The firmware upgrade file size is too big.
- The firmware image file is not valid.
- A valid firmware image has not been loaded.
- The flash process could not be started.
- IMAGE\_LOCATION must not be blank.
- User does not have correct privilege for action.
- Logged-in user does not have required privilege for this command.

## **GET\_FW\_VERSION**

The GET\_FW\_VERSION command returns the version and date of the firmware on the iLO.

Example:

```
<RIBCL VERSION="2.0">
  <LOGIN USER_LOGIN="adminname" PASSWORD="password">
    <RIB_INFO MODE="read">
      <GET_FW_VERSION/>
    </RIB_INFO>
  </LOGIN>
</RIBCL>
```

### **GET\_FW\_VERSION Parameters**

There are no parameters for this command.

### **GET\_FW\_VERSION Runtime Errors**

There are no errors for this command.

## GET\_FW\_VERSION Return Messages

The following information is returned within the response:

```
<GET_FW_VERSION
  FIRMWARE_VERSION = <firmware version>
  FIRMWARE_DATE = <firmware date>
  MANAGEMENT_PROCESSOR = <management processor type>
/>
```

## HOTKEY\_CONFIG

The HOTKEY\_CONFIG command configures the Remote Console hot key settings on the iLO. The HOTKEY\_CONFIG command must be displayed within a RIB\_INFO element, and RIB\_INFO must be in write mode. All of the subelements of the command are optional. The user must be logged in with the configure iLO privilege to execute this command.

Uppercase letters are not supported, and they will be converted automatically to lowercase. If either a double quote or a single quote is used, it must be different from the delimiter. CTRL subelements that are not present are not modified. Specifying a blank string removes the current value.

Example:

```
<RIBCL VERSION="2.0">
  <LOGIN USER_LOGIN="adminname" PASSWORD="password">
    <RIB_INFO MODE="write">
      <HOTKEY_CONFIG>
        <CTRL_T value="CTRL,ALT,ESC"/>
        <CTRL_U value="L_SHIFT,F10,F12"/>
        <CTRL_V value=""/>
        <CTRL_Y value=""/>
        <CTRL_X value=""/>
        <CTRL_Y value=""/>
      </HOTKEY_CONFIG>
    </RIB_INFO>
  </LOGIN>
</RIBCL>
```

## HOTKEY\_CONFIG Parameters

CTRL\_T specifies settings for the CTRL\_T hot key. The settings need to be separated by commas. For example, CTRL\_T="CTRL,ALT,ESC." Up to five keystrokes can be configured for each hot key.

CTRL\_U specifies settings for the CTRL\_U hot key. The settings need to be separated by commas. For example, CTRL\_U="CTRL,ALT,ESC." Up to five keystrokes can be configured for each hot key.

CTRL\_V specifies settings for the CTRL\_V hot key. The settings need to be separated by commas. For example, CTRL\_V="CTRL,ALT,ESC." Up to five keystrokes can be configured for each hot key.

CTRL\_W specifies settings for the CTRL\_W hot key. The settings need to be separated by commas. For example, CTRL\_W="CTRL,ALT,ESC." Up to five keystrokes can be configured for each hot key.

CTRL\_X specifies settings for the CTRL\_X hot key. The settings need to be separated by commas. For example, CTRL\_X="CTRL,ALT,ESC." Up to five keystrokes can be configured for each hot key.

CTRL\_Y specifies settings for the CTRL\_Y hot key. The settings need to be separated by commas. For example, CTRL\_Y="CTRL,ALT,ESC." Up to five keystrokes can be configured for each hot key.

## HOTKEY\_CONFIG Runtime Errors

The possible HOTKEY\_CONFIG error messages include:

- RIB information is open for read-only access. Write access is required for this operation.
- The hot key parameter specified is not valid.
- Invalid number of hot keys. The maximum allowed is five.
- User does not have correct privilege for action.

## LICENSE

The LICENSE command activates or deactivates the iLO advanced features. If the server is a ProLiant BL p-Class server, there is no need for a licensing key because the advance features are already activated.

The LICENSE command must be displayed within a RIB\_INFO element and RIB\_INFO must be in write mode. The user must be logged in with the Configure iLO privilege. All of the sub-elements of the command are optional.

Example:

```
<RIBCL VERSION="2.0">
  <LOGIN USER_LOGIN="adminname" PASSWORD="password">
    <RIB_INFO MODE="write">
      <LICENSE>
        <ACTIVATE KEY="1111122222333334444455555"/>
      </LICENSE>
    </RIB_INFO>
  </LOGIN>
</RIBCL>
```

### LICENSE Parameters

ACTIVATE followed by a valid KEY value signals the activation of the iLO advanced pack licensing.

KEY specifies the license key value. The key should be entered as one continuous string. Commas, periods, or other characters should not separate the key value. The key will only accept 25 characters; other characters entered to separate key values will be interpreted as a part of the key and result in the wrong key being entered.

DEACTIVATE signals the deactivation of the iLO advanced pack licensing.

### LICENSE Runtime Errors

The possible LICENSE error messages include:

- License key error.

- License is already active.
- User does not have correct privilege for action.

## RACK\_INFO

The RACK\_INFO command is used to tell the firmware that the ProLiant BL p-Class rack information is about to be changed. This command block is only valid on rack servers. The user must be logged in with the Configure iLO privilege.

Example:

```
<RACK_INFO MODE="read">
..... RACK_INFO commands .....
</RACK_INFO>
```

## RACK\_INFO Parameters

MODE is a specific string parameter with a maximum length of 10 characters that specifies what you intend to do with the user information. Valid arguments are "read" and "write."

If it is open in write mode, then both reading and writing are enabled. If it is open in read mode, then this instance will not be able to perform any rack modifications. It is case insensitive. This parameter must never be blank.

## RACK\_INFO Runtime Errors

The possible RACK\_INFO error messages include:

- Invalid Mode.
- Server is not a rack server; rack commands do not apply.



## MOD\_BLADE\_RACK

The MOD\_BLADE\_RACK is used to modify certain ProLiant BL p-Class rack settings. The MOD\_BLADE\_RACK must be displayed within a RACK\_INFO element and RACK\_INFO must be in write mode. The user must be logged-in with the Configure Rack privilege. All of the sub-elements are optional. If any sub-element is left out, then the current setting is preserved.

Example:

```
<RIBCL VERSION="2.0">
  <LOGIN USER_LOGIN="userlogin" PASSWORD="password">
    <RACK_INFO MODE="write">
      <MOD_BLADE_RACK>
        <RACK_NAME value="CPQ_Rack_1"/>
        <ENCLOSURE_NAME value="CPQ_Enclosure_1"/>
        <BAY_NAME value="CPQ_Bay_5"/>
        <FACILITY_PWR_SOURCE value="Yes"/>
        <RACK_AUTO_PWR value="Yes"/>
        <LOG_RACK_ALERTS value="Yes"/>
      </MOD_BLADE_RACK>
    </RACK_INFO>
  </LOGIN>
</RIBCL>
```

### MOD\_BLADE\_RACK Parameters

RACK\_NAME is used to logically group together the components that comprise a single rack. When changed, the rack name is communicated to all other components connected in a rack. The name is used when logging and alerting to assist in identifying the component. The RACK\_NAME can be no more than 31 characters.

ENCLOSURE\_NAME is used to logically group together the ProLiant BL p-Class servers that comprise a single enclosure. When changed, the enclosure name is communicated to all other blade servers connected in the same enclosure. The name is used when logging and alerting to assist in identifying the component. The ENCLOSURE\_NAME can be no more than 31 characters.

BAY\_NAME is used to assist in identifying a component or a components function. The name is used when logging and alerting to assist in identifying the component. The BAY\_NAME can be no more than 31 characters.

FACILITY\_PWR\_SOURCE determines the source of power for the blade servers. A value of "Yes" directs the server to use facility power and a value of "No" directs the server to use the server blade power supplies.

RACK\_AUTO\_PWR determines if the blade server should automatically power up. A value of "Yes" causes the blade server to automatically power up and begin normal booting process if power is available. A value of "No" requires the blade server to be manually powered on.

LOG\_RACK\_ALERTS determines if alerts from the rack infrastructure should be logged. A value of "Yes" enables rack alerts to be logged in the IML log. A value of "No" disables the logging of rack alerts in the IML log.

## **MOD\_BLADE\_RACK Runtime Errors**

The possible MOD\_BLADE\_RACK error messages include:

- Rack information is open for read-only access. Write access is required for this operation.
- Rack Name too long.
- Enclosure Name too long.
- Bay Name too long.
- User does not have correct privilege for action.

## **GET\_TOPOLOGY**

The GET\_TOPOLOGY command requests that iLO return the rack topology of the current rack. The GET\_TOPOLOGY command must be displayed within a RACK\_INFO element.

Example:

```
<RIBCL VERSION="2.0">
```

```

<LOGIN USER_LOGIN="adminname" PASSWORD="password">
<RACK_INFO MODE="read">
  <GET_TOPOLOGY/>
</RACK_INFO>
</LOGIN>
</RIBCL>

```

## GET\_TOPOLOGY Parameters

There are no parameters for this command.

## GET\_TOPOLOGY Return Message

An example of a successful request follows:

```

<RK_TPLGY CNT="3">
<RUID>xxxxxx</RUID>
<ICMB ADDR="0xAA55" MFG="232" PROD_ID="NNN" SER="123"
NAME="Power_1">
<LEFT/>
<RIGHT ADDR="0xAB66" SER="123" NAME="Server_1"/>
</ICMB>
<ICMB ADDR="0xAB66" MFG="232" PROD_ID="NNN" SER="456"
NAME="Server_1">
<LEFT ADDR="0xAA55" SER="123" NAME="Power_1"/>
<RIGHT ADDR="0xAC77" SER="123" NAME="Power_2"/>
</ICMB>
<ICMB ADDR="0xAC77" MFG="232" PROD_ID="NNN" SER="789"
NAME="Power_2">
<RIGHT/>
</ICMB>
</RK_TPLGY>

```

## SERVER\_INFO

The SERVER\_INFO command tells the firmware that the configuration of the iLO is about to be changed.

Example:

```

<SERVER_INFO MODE="read">

```

```
..... SERVER_INFO commands .....  
</SERVER_INFO>
```

## SERVER\_INFO Parameter

MODE is a specific string parameter that has a maximum length of 10 characters. It tells the iLO what you intend to do with the server information. Valid arguments are "read" and "write." If the parameter is open in write mode, then both reading and writing are enabled. If it is open in read mode, the user cannot perform any server actions. If this parameter is not specified, "read" is assumed.

## SERVER\_INFO Runtime Error

A possible SERVER\_INFO error is: Mode parameter must not be blank.

## GET\_HOST\_POWER\_STATUS

The GET\_HOST\_POWER\_STATUS command displays the server power state from the Virtual Power Button cable. The GET\_HOST\_POWER\_STATUS command must be displayed within a SERVER\_INFO element, and SERVER\_INFO must be in write mode.

Example:

```
<RIBCL VERSION="2.0">  
  <LOGIN USER_LOGIN="adminname" PASSWORD="password">  
    <SERVER_INFO MODE="write">  
      <GET_HOST_POWER_STATUS/>  
    </SERVER_INFO>  
  </LOGIN>  
</RIBCL>
```

## GET\_HOST\_POWER\_STATUS Parameters

There are no parameters for this command.

## GET\_HOST\_POWER\_STATUS Runtime Errors

The possible GET\_HOST\_POWER\_STATUS error messages include:

- Host power is OFF.
- Host power is ON.

## GET\_HOST\_POWER\_STATUS Return Messages

The following information is returned within the response:

```
<GET_HOST_POWER
  HOST_POWER="OFF"
/>
```

## SET\_HOST\_POWER

The SET\_HOST\_POWER command sets the Virtual Power Button feature. This feature is used to turn the server on or off if the feature is supported. The SET\_HOST\_POWER command must be displayed within a SERVER\_INFO element, and SERVER\_INFO must be in write mode. The user must be logged in with reset server privilege to execute this command.

Example:

```
<RIBCL VERSION="2.0">
  <LOGIN USER_LOGIN="adminname" PASSWORD="password">
    <SERVER_INFO MODE="write">
      <SET_HOST_POWER HOST_POWER="Yes"/>
    </SERVER_INFO>
  </LOGIN>
</RIBCL>
```

## SET\_HOST\_POWER Parameters

HOST\_POWER enables or disables the Virtual Power Button. The possible values are "Yes" or "No."

## SET\_HOST\_POWER Runtime Errors

The possible SET\_HOST\_POWER error messages include:

- Server information is open for read-only access. Write access is required for this operation.
- Virtual Power Button feature is not supported on this server.
- Host power is already ON.
- Host power is already OFF.
- User does not have correct privilege for action.
- Logged-in user does not have required privilege for this command.

## RESET\_SERVER

The RESET\_SERVER command resets the server if the server is turned on. The RESET\_SERVER command must be displayed within a SERVER\_INFO element, and SERVER\_INFO must be in write mode. The user must be logged in with reset server privilege to execute this command.

Example:

```
<RIBCL VERSION="2.0">
  <LOGIN USER_LOGIN="adminname" PASSWORD="password">
    <SERVER_INFO MODE="write">
      <RESET_SERVER/>
    </SERVER_INFO>
  </LOGIN>
</RIBCL>
```

## RESET\_SERVER Parameters

There are no parameters for this command.

## RESET\_SERVER Errors

The possible RESET\_SERVER error messages include:

- Server information is open for read-only access. Write access is required for this operation.
- Server is currently powered off.
- User does not have correct privilege for action.
- Logged-in user does not have required privilege for this command.

## GET\_UID\_STATUS

The UID\_STATUS command provides the status of the server UID light.

Example:

```
<RIBCL VERSION="2.0">
  <LOGIN USER_LOGIN="adminname" PASSWORD="password">
    <SERVER_INFO MODE="write">
      <GET_UID_STATUS />
    </SERVER_INFO>
  </LOGIN>
</RIBCL>
```

## GET\_UID\_STATUS Parameters

There are no parameters for this command.

## GET\_UID\_STATUS Response

The following information is returned within the response:

```
<GET_UID_STATUS
  UID="OFF"
/>
```

## UID\_CONTROL

The UID\_CONTROL command turns the server UID light off or on. The UID\_CONTROL command must be displayed within a SERVER\_INFO element and SERVER\_INFO must be in write mode.

Example:

```
<RIBCL VERSION="2.0">
  <LOGIN USER_LOGIN="adminname" PASSWORD="password">
    <SERVER_INFO MODE="write">
      <UID_CONTROL UID="Yes"/>
    </SERVER_INFO>
  </LOGIN>
</RIBCL>
```

## **UID\_CONTROL Parameters**

UID determines the state of the UID. A value of "Yes" turns the UID light on, and a value of "No" turns the UID light off.

## **UID\_CONTROL Errors**

The possible UID\_CONTROL error messages include:

- UID is already ON.
- UID is already OFF.



# Integrated Lights-Out Parameters

## In This Section

Integrated Lights-Out Parameters Table.....	207
Server Identification Parameters .....	211
User Administration Parameters.....	212
Global Settings Parameters.....	214
Network Settings Parameters.....	216
Directory Settings Parameters .....	219
SNMP/Insight Manager Settings Parameters .....	221
ProLiant BL p-Class Parameters .....	223
iLO Advanced License Activation Settings .....	225

## Integrated Lights-Out Parameters Table

You can record your settings in the "Your Value" column of the table.

Parameters	Default Value or Setting	Your Value
<b>Server Identification</b>		
PCI Resources	Set by the bios	
Server Name		
Server ID		
Serial Number	iLOXXXXXXXXXXXXX	
Firmware Version	XX.XX	
Firmware Date	mm/dd/yyyy	
<b>User Administration</b>		
User Name	Administrator	
Login Name	Administrator	
Password	A random, eight-character alphanumeric string that is factory assigned	
Administer User Accounts	Yes	
Remote Console Access	Yes	
Virtual Power and Reset	Yes	
Virtual Media	Yes	
Configure iLO Settings	Yes	
<b>Global Settings</b>		
Enable Lights-Out Functionality	Yes	
Idle Connection Timeout (minutes)	30 minutes	
Web Server Non-SSL Port	80	
Web Server SSL Port	443	
Virtual Media Port	17988	
Remote Console Port	23	
Enable iLO ROM-Based Setup Utility	Yes	

Parameters	Default Value or Setting	Your Value
Require Login for iLO RBSU	No	
Minimum Password Length	8	
<b>Network Settings</b>		
Enable NIC	Yes	
Transceiver Speed Autoselect	Yes	
Speed	N/A (Autoselect)	
Duplex	N/A (Autoselect)	
Enable DHCP	Yes	
Use DHCP Supplied Gateway	Yes	
Use DHCP Supplied DNS Servers	Yes	
Use DHCP Supplied WINS Servers	Yes	
Use DHCP Supplied Static Routes	Yes	
Use DHCP Supplied Domain Name	Yes	
Register With WINS Server	N/A (DHCP)	
Register With DNS Server	N/A (DHCP)	
Ping Gateway on Startup	No	
iLO IP Address	N/A (DHCP)	
iLO Subnet Mask	N/A (DHCP)	
iLO Gateway IP Address	N/A (DHCP)	
iLO Subsystem Name	iLOXXXXXXXXXXXX, where the 12 Xs are the server serial number (assigned at the factory)	
Domain Name	N/A (DHCP)	
DHCP Server	N/A (DHCP)	

Parameters	Default Value or Setting	Your Value
Primary, Secondary, and Tertiary DNS Server	N/A (DHCP)	
Primary and Secondary WINS Server	N/A (DHCP)	
Static Routes #1, #2, #3	N/A for both the Destination and Gateway address (DHCP)	
<b>SNMP/Insight Manager Settings</b>		
SNMP Alert Destination(s)	No	
Enable iLO SNMP Alerts	No	
Forward Insight Manager Agent SNMP Alerts	No	
Insight Manager Web Agent URL		
Level of Data Returned	Medium	
<LOM_short_name> Advanced License Activation		
iLO Advanced Pack License Key	No	
<b>BL p-Class</b>		
Rack Name	Provided by rack	
Enclosure Name	Provided by rack	
Bay Name	Bay X (where X is the bay number in which the blade server is located)	
Bay	Provided by rack	
Rack Serial Number	Provided by rack	
Enclosure Serial Number	Provided by rack	
Blade Serial Number	Provided by blade server	
Power Source	Rack Provides Power	
Enable Automatic Power On	On	

Parameters	Default Value or Setting	Your Value
Enable Rack Alert Forwarding	On	
Enable Rack Alert Logging (IML)	On	
<b>Directory Settings</b>		
Directory Authentication	Disabled	
Directory Server Address	0.0.0.0	
Directory Server LDAP Port	636	
LOM Object Distinguished Name		
LOM Object Password		
Directory User Context 1		
Directory User Context 2		
Directory User Context 3		

## Server Identification Parameters

The following parameters provide information about the host server.

### PCI Resources

This field shows the interrupt reserved for PCI resources. The value is set by the bios.

### Server Name

If the Insight Management agents are being used with the host server operating system, they will provide iLO with the server name.

## Serial Number

This is the serial number of iLO. The number is displayed for your information. You cannot alter this number.

## Firmware Version

This is the version number of the iLO firmware. You cannot alter this value.

## Firmware Date

This is the date of the firmware version resident on iLO in *mm/dd/yyyy* format. It is displayed for your information only and cannot be altered.

## User Administration Parameters

The User Administration section enables you to define the users currently configured for access to iLO. Up to 12 users can be specified. User configurations can be added, deleted, or modified by using the Web interface.

### User Name

This parameter is the user's real name as it is displayed in the user list and event log. It is not the name used to log in. The maximum length of the user name is 39 characters.

### Login Name

This is a case-sensitive name that the user must provide to log in to iLO.

## Password

This is a case-sensitive password that the user must provide to log in to iLO. In **Security Options**, the minimum password length can be assigned. The minimum password can be from 0 to 39 characters. The default minimum password length is eight characters. You must enter the password twice for verification.

## Administer User Accounts

This privilege allows a user to add, modify, and delete user accounts. It also allows the user to alter privileges for all users, including granting all permissions to a user.

## Remote Console Access

This privilege allows a user to remotely manage the Remote Console of a managed system, including video, keyboard, and mouse controls.

## Virtual Power and Reset

This privilege allows a user to power-cycle or reset the host platform.

## Virtual Media

This privilege allows a user to use virtual media on the host platform.

## Configure iLO Settings

This privilege enables a user to configure most iLO settings, including security settings. It does not include user account administration.

After iLO is correctly configured, revoking this privilege from all users prevents reconfiguration. A user with the Administer User Accounts privilege can enable or disable this privilege. iLO can also be reconfigured if iLO RBSU is enabled.

## Global Settings Parameters

The Global Settings section enables you to define the overall security level for iLO. These settings are applied globally, regardless of the individual user settings.

### Idle Connection Timeout (Minutes)

This option specifies the interval of user inactivity, in minutes, before the Web server and Remote Console session are automatically terminated.

### Enable Lights-Out Functionality

This option allows connection to iLO. If disabled, all connections to iLO are prevented. The default setting is **Yes**.

### Enable iLO ROM-Based Setup Utility

This option enables a user with access (physical or virtual) to the host to configure iLO for that system using the iLO RBSU. RBSU is invoked when the host system reboots and performs POST. The default setting is Yes. You can restrict RBSU access to authorized users using the **Require Login for iLO RBSU** setting.

**NOTE:** If the physical security jumper is set, the RBSU prompt displays during reboot.

### Require Login for iLO RBSU

This option specifies whether the user is required to provide a login name and password to access the iLO RBSU. The default setting is No.



## Remote Console Port Configuration

This option enables or disables configuring of the port address. Setting this option to **Enabled** allows Telnet and Remote Console applet access. Setting this option to **Disabled** turns off both Telnet and Remote Console applet access. **Remote Console Data Encryption** must be set to **No** to use Telnet to access the text Remote Console.

## Remote Console Data Encryption

This option enables encryption of Remote Console data. If using a standard Telnet client to access the iLO, this setting must be set to **No**.

## SSL Encryption Strength

This option displays the current cipher strength setting. The most secure is 128-bit (High).

## Current Cipher

This option displays the encryption algorithm currently being used to protect data during transmission between the browser and the iLO.

## Web Server Non-SSL Port

The embedded Web server in iLO is configured by default to use port 80 for unencrypted communications. This port setting is configurable in the **Global Settings** option of the **Administration** tab.

## Web Server SSL Port

The embedded Web server in iLO is configured by default to use port 443 for encrypted communications. This port setting is configurable in the **Global Settings** option of the **Administration** tab.

## Virtual Media Port

The Virtual Media support in iLO uses a configurable port for its communications. This port can be set in the **Global Settings** option of the **Administration** tab. The default setting is to use port 17988.

## Remote Console Port

The iLO Remote Console is configured by default to use port 23 for Remote Console communications. This port setting is configurable in the **Global Settings** option of the **Administration** tab.

## Minimum Password Length

This option specifies the minimum number of characters allowed when a user password is set or changed. The character length can be set at a value from 0 to 39. The default setting is eight characters.

## Network Settings Parameters

The following parameters provide information about the iLO network settings.

### Enable NIC

This parameter enables the NIC to reflect the state of iLO. The default setting for the NIC is **Yes**, which is enabled. If DHCP is disabled, you must assign a static IP address to iLO. Assign the IP address using the iLO IP Address parameter described in this section.

### Transceiver Speed Autoselect

Autoselect detects the interface speed and sets the interface to operate at 10 Mbps or 100 Mbps and at half or full duplex. If necessary, this parameter can be set to manual to allow manual adjustment of speed and duplex settings.

## Speed

Use this setting to assign 10-Mbps or 100-Mbps connect speeds if Transceiver Speed Autoselect is not enabled.

## Duplex

Use this setting to assign half or full duplex to the NIC if Transceiver Speed Autoselect is not enabled.

## DNS/DHCP

iLO comes preset from HP with DNS/DHCP enabled. To disable DHCP, you must use the iLO RBSU.

**NOTE:** If you disable DHCP, you will have to manually set up the IP address and the subnet mask using the iLO RBSU.

If DHCP is enabled, the following settings are also enabled:

- Use DHCP Supplied Gateway
- Use DHCP Supplied DNS Servers
- Use DHCP Supplied WINS Servers
- Use DHCP Supplied Static Routes
- Use DHCP Supplied DNS Name

If DHCP has been disabled, these settings may have to be assigned.

## Registering with WINS Server

iLO automatically registers with a WINS server. The default setting is **Yes**. By default, WINS server addresses are assigned by DHCP.

## Registering with DNS Server

iLO automatically registers with a DNS server. The default setting is **Yes**. By default, DNS server addresses are assigned by DHCP.

## Ping Gateway on Startup

This option causes iLO to send four ICMP echo request packets to the gateway when iLO initializes. This option ensures that the ARP cache entry for iLO is current on the router responsible for routing packets to and from iLO.

## iLO IP Address

Use this parameter to assign a static IP address to iLO on your network. By default, the IP address is assigned by DHCP.

## iLO Subnet Mask

Use the subnet mask parameter to assign the subnet mask for the default gateway. By default, the subnet mask is assigned by DHCP.

## iLO Gateway IP Address

Use the gateway parameter to assign the IP address of the network router that connects the iLO subnet to another subnet where the management console resides. The default gateway is assigned by DHCP.

## iLO Subsystem Name

iLO comes preset with a DNS/WINS name. The DNS/WINS name is "iLO" plus the serial number of the server. This name also is displayed on the tag attached to the bracket of iLO. You can change this value.

## Domain Name

Enter the name of the domain that iLO will participate in. By default, the domain name is assigned by DHCP.

## DHCP Server

This setting is automatically detected if DHCP is set to **Yes**. You cannot change this setting.

## Primary, Secondary, and Tertiary DNS Server

Use this parameter to assign a unique DNS server IP address on the network. By default, the primary, secondary, and tertiary DNS servers are assigned by DHCP.

## Primary and Secondary WINS Server

Use this parameter to assign a unique WINS server IP address on the network. By default, the primary and secondary WINS servers are assigned by DHCP.

## Static Route #1, #2, #3

Use this parameter to assign a unique static route destination and gateway IP address pair on the network. Up to three static route pairs can be assigned. By default, the static routes are assigned by DHCP.

## Directory Settings Parameters

The following parameters provide information about the Directory Settings.

### Directory Authentication

This parameter enables or disables directory authentication. If directory support is properly configured, this enables user login to iLO using directory credentials.

## Directory Server Address

This parameter specifies the Directory Server DNS name or IP address. HP recommends using a DNS name or multi-host DNS name. If an IP address is used, the directory will not be available if that server is down.

## Directory Server LDAP Port

This option sets the port number used to connect to the directory server. The SSL secured LDAP port number is 636.

## LOM Object Distinguished Name

This option specifies the unique name for the iLO in the directory. LOM Object Distinguished Names are limited to 256 characters.

## LOM Object Password

This parameter specifies the password for the iLO object to access the directory. LOM Object Passwords are limited to 39 characters.

**NOTE:** At this time, the LOM Object Password field is not used. This field is to provide forward compatibility with future firmware releases.

## Directory User Context 1, Directory User Context 2, Directory User Context 3

This parameter enables you to specify up to three searchable contexts used to locate the user when the user is trying to authenticate using the directory. Directory User Contexts are limited to 128 characters each. Directory User Contexts enable you to specify directory user containers that are automatically searched when an iLO login is attempted. This eliminates the requirement of entering a fully distinguished user name at the login screen. For example, the search context, "ou=lights out devices,o=corp" would allow the user "cn=manager,ou=lights out devices,o=corp" to login to iLO using just "manager." Active Directory allows an additional search context format, "@hostname" for example, "@directory.corp."

## Testing Directory Settings

After updating the directory settings, click the **Apply Settings** button to store the settings. When the **Test Settings** button is enabled, you can validate the current directory settings. To test these settings:

1. Be sure the **Enable Directory Authentication** setting is enabled.
2. Click the **Test Settings** button.
3. Enter the fully distinguished name and password of the user used to add iLO to the directory server in the **Directory Administrator Distinguished Name** and **Directory Administrator Password** fields.
4. Enter the credentials of an expected directory-based iLO User account in the **Test User Name** and **Test User Password** fields.
5. Click the **Start Test** button.

A series of tests will begin, and the page will automatically refresh as the tests progress. View the test status to diagnose the results, and consult the help page for specific test result details. The test results are cleared if any directory settings are changed, if iLO is reset, or if the tests are restarted.

## SNMP/Insight Manager Settings Parameters

iLO supports SNMP settings on a device level. These parameters are not designated on a per-user basis but are specific to iLO.

### SNMP Alert Destinations

Enter the IP address of the remote management PC that will receive SNMP trap alerts from iLO. Up to three IP addresses can be designated to receive SNMP alerts.

## Enable iLO SNMP Alerts

These alert conditions are detected by iLO and are independent of the host server operating system. These alerts can be Insight Manager SNMP traps. These alerts include major events, such as remote server power outages or server resets. They also include iLO events, such as security disabled or failed login attempt. iLO forwards the alerts to an Insight Manager 7 console using the destinations provided. The default setting is Yes.

## Forward Insight Manager Agent SNMP Alerts

These alerts are generated by the Insight Management agents, which are provided for each supported network operating system. The agents must be installed on the host server to receive these alerts. These alerts are sent to Insight Manager 7 clients on the network and are forwarded asynchronously by iLO to the IP addresses that have been configured to receive them. The default setting is Yes.

## Insight Manager Web Agent URL

The Insight Manager Web Agent URL option enables you to enter the IP address or the DNS name of the host server on which the Insight Manager Web Agents are running. Entering this data in the field provided enables iLO to create a link from the iLO Web pages to the pages of the Web Agent.

## Level of Data Returned

The Level of Data Returned option regulates how much data is returned to an anonymous request for iLO information from Insight Manager 7. All settings, except the None Data Level, provide sufficient data to allow integration with Insight Manager 7. The Medium and High settings enable Insight Manager 7 to associate the management processor with the host server. The None Data Level prevents iLO from responding to the Insight Manager 7 requests. The default setting is Medium.



## ProLiant BL p-Class Parameters

The following parameters provide information about the ProLiant BL p-Class settings.

### Rack Name

The rack name is used to logically group together the components that comprise a single rack. When changed, the rack name is communicated to all other components connected in a rack. The name is used when logging and alerting to assist in identifying the component.

### Enclosure Name

The enclosure name is used to logically group together the server blades that comprise a single enclosure. When changed, the enclosure name is communicated to all other server blades connected in the same enclosure. The name is used when logging and alerting to assist in identifying the component.

### Bay Name

The bay name is used when logging and alerting to assist in identifying a component or its function.

### Bay

The ProLiant BL p-Class enclosure can support one to eight server blades. The bays are numbered from left to right starting with 1 and finishing with 8. The bay number is used to assist in physically identifying the faulty server blade or other error conditions. This information is for viewing only.

## Rack Serial Number

The rack serial number identifies the components in the rack as a logical grouping. The serial number is determined during power-up of the various components to create a unique rack serial number. Switching components (server blade enclosure or power supplies) alters the rack serial number.

## Enclosure Serial Number

The enclosure serial number identifies the particular server blade enclosure in which a server blade resides.

## Blade Serial Number

The blade serial number identifies the serial number for the server blade product.

## Power Source

The server blade enclosure can be installed in a rack by using one of two configurations:

- The server blade power supplies can be used to convert normal AC facility power to 48 V DC to power the rack. In this configuration, select the power source as **Rack Provides Power**. This setting allows each server blade, enclosure, and power supply to communicate power requirements to ensure proper power consumption without risking power failures.
- If the facility can provide 48 V DC power directly, without the need for the provided power supplies, then select **Facility Provides 48V**. Each server blade will not be required to communicate with the infrastructure for power when powering on or off.

**NOTE:** It is essential that proper power sizing requirements be performed to ensure sufficient power for all the server blades and other components of the rack.

## Enable Automatic Power On

Each server blade can be configured to automatically power on when inserted into the enclosure. Depending on the Power Source setting, the server blade communicates with the rack to determine if enough power is available to power on. If the power is available, then the server blade automatically powers on and begins the normal server booting process.

## iLO Advanced License Activation Settings

The following parameter provides information about the licensing of the iLO Advanced Features.

### iLO Advanced Pack License Key

The iLO Advanced Pack License Key option is used to enable the iLO Advanced Features including Graphical Remote Console, virtual media (floppy and CD\_ROM), and directory support . Enter the 25-character key in this field to enable the features.

---

# Troubleshooting Integrated Lights-Out

## In This Section

Minimum Requirements .....	227
Troubleshooting Alert and Trap Problems .....	228
iLO POST LED Indicators .....	229
Hardware and Software Link-Related Issues .....	231

## Minimum Requirements

iLO has the following minimum requirements:

- Windows® clients
  - Windows® 2000
  - Microsoft® Internet Explorer 5.5 with SP2 with 128-bit encryption
  - Java 1.3.1 JVM or later
- Linux clients
  - Red Hat 7.3
  - Netscape 7.x or Mozilla 1.2.1 with 128-bit encryption
  - Java 1.4.1 JVM or later

To download the recommended JVM for your system configuration, refer to the HP website (<http://www.hp.com/servers/manage/jvm>).

**NOTE:** You will be redirected from the main site to the java.sun.com site. HP recommends using the version specified in the Remote Console help pages. You can obtain the specified version for Internet Explorer either from the java.sun site or on the Management CD.

## Troubleshooting Alert and Trap Problems

Alert	Explanation
Test Trap	This trap is generated by a user through the Web configuration page.
Server Power Outage	Server has lost power.
Server Reset	Server has been reset.
Failed Login Attempt	Remote user login attempt failed.
General Error	This is an error condition that is not predefined by the hard coded MIB.
Logs	Circular log has been overrun.
Security Override Switch Changed: On/Off	The state of the Security Override Switch has changed (On/Off).
Rack Server Power On Failed	The server was unable to power on because the BL p-Class rack indicated that insufficient power was available to power on the server.
Rack Server Power On Manual Override	The server was manually forced by the customer to power on despite the BL p-Class reporting insufficient power.
Rack Name Changed	The name of the ProLiant BL p-Class rack was changed.

### Inability to Receive Insight Manager 7 Alarms (SNMP Traps) from iLO

A user with the Configure iLO Settings privilege must connect to iLO to configure SNMP trap parameters. When connected to iLO, be sure that the correct alert types and trap destinations are enabled in the **SNMP/Insight Manager Settings** screen of the iLO console application.

### iLO Security Override Switch

The iLO Security Override Switch allows emergency access to the administrator with physical control over the server system board. Setting the iLO Security Override Switch allows login access, with all privileges, without a user ID and password.

The iLO Security Override Switch is located inside the server and cannot be accessed without opening the server enclosure. To set the iLO Security Override Switch, the server must be powered off and disconnected from the power source. Set the switch and then power on the server. Reverse the procedure to clear the iLO Security Override Switch.

A warning message is displayed on the iLO Web pages, indicating that the iLO Security Override Switch is currently in use. An iLO log entry is added recording the use of the iLO Security Override Switch. An SNMP alert may also be sent upon setting or clearing the iLO Security Override Switch.

In the unlikely event that it is necessary, setting the iLO Security Override Switch also enables you to flash the iLO boot block. The boot block is exposed until iLO is reset. HP recommends that you disconnect iLO from the network until the reset is complete.

Depending on the server, the iLO Security Override Switch may be a single jumper or it may be a specific switch position on a dip switch panel. To access the iLO Security Override Switch, refer to the server documentation.

## iLO POST LED Indicators

During the initial boot of iLO, the POST LED indicators flash to display the progress through the iLO boot process. After the boot process is complete, the heartbeat (HB) LED flashes every second. LED 7 also flashes intermittently during normal operation.

The LED indicators (1 through 6) light up after the system has booted to indicate a hardware failure. If a hardware failure is detected, reset iLO. For the location of the LED indicators, refer to the server documentation.

A runtime failure of iLO is indicated by HB and LED 7 remaining in either the On or Off state constantly. A runtime failure of iLO may also be indicated by a repeated flashing pattern on all eight LEDs. If a runtime error occurs, reset iLO.

The LED indicators have the following assignments:

HB	7	6	5	4	3	2	1
----	---	---	---	---	---	---	---

LED Indicators	POST Code (Activity Completed)	Description	Failure Indicates
None	00	Set up chip selects.	
1 or 2	02—Normal operation	Determine platform.	
2 and 1	03	Set RUNMAP bit.	
3	04	Initialize SDRAM controller.	
3 and 2	06	Activate the I cache.	
3, 2, and 1	07	Initialize (only) the D cache.	
4	08	Copy secondary loader to RAM.	Could not copy secondary loader.
4 and 1	09	Verify secondary loader.	Did not execute secondary loader.
4 and 2	0a	Begin secondary loader.	SDRAM memory test failed.
4, 2, and 1	0b	Copy ROM to RAM.	Could not copy boot block.
4 and 3	0c	Verify ROM image in RAM.	Boot block failed to execute.
4, 3, and 1	0d	Boot Block Main started.	Boot block could not find a valid image.
None		Start C Run time initialization.	
4, 3, and 2	0e	Main() has received control.	Main self-test failed.
Varies	Varies	Each subsystem may self-test.	
4, 3, 2, and 1	0f	Start ThreadX.	RTOS startup failed.
None	00	Main_init() completed.	Subsystem startup failed.

LED Indicators	POST Code (Activity Completed)	Description	Failure Indicates
HB and 7		Blinks as the iLO processor executes firmware code. It does not change the value of the lower six LEDs.	

The iLO microprocessor firmware includes code that makes consistency checks. If any of these checks fail, the microprocessor executes the FEH. The FEH presents information using the iLO POST LED indicators. The FEH codes are distinguished by the alternating flashing pattern of the number 99 plus the remainder of the error code.

FEH Code	Consistency Check	Explanation
9902	TXAPICHK	An RTOS function was called with an inappropriate value, or was called from an inappropriate caller.
9903	TXCONTEXT	The saved context of one or more threads has been corrupted.
9905	TRAP	A stack probe failed, return address is invalid, or illegal trap instruction has been detected.
9966	NMIWR	An unexpected write to low memory has occurred.
99C1	CHKNUL	The reset vector has been modified.

## Hardware and Software Link-Related Issues

The following sections discuss items to be aware of when attempting to resolve hardware or software link-related issues.

### Hardware

iLO uses standard Ethernet cabling, which includes CAT5 UTP with RJ-45 connectors. Straight-through cabling is necessary for a hardware link to a standard Ethernet hub. Use a crossover cable for a direct PC connection.



## Software

The iLO Management Port must be connected to a network that is connected to a DHCP server, and iLO must be on the network before power is applied. DHCP sends a request soon after power is applied. If the DHCP request is not answered when iLO first boots, then it will reissue the request at 90-second intervals.

The DHCP server must be configured to supply DNS and WINS name resolution. iLO can be configured to work with a static IP address either in the F8 option ROM setup or from the **Network Settings** Web page.

The default DNS name appears on the network settings tag and can be used to locate iLO without knowing the assigned IP address.

If a direct connection to a PC is used, then a static IP address must be used because there is no DHCP server on the link.

Within the iLO RBSU, you may press the **F1** key inside the **DNS/DHCP** page for advanced options to view the status of iLO DHCP requests.

## Login Issues

Use the following information when attempting to resolve login issues:

- The default login is on the network settings tag.
- If you forget your password, an administrator with the Administer User Accounts privilege can reset it for you.
- If an administrator forgets his or her password, the administrator must use the Security Override Switch.
- Check for standard problems, such as:
  - Is the password complying with password restrictions? For example, are there case-sensitive characters in the password?
  - Is an unsupported browser being used?

## Login Name and Password Not Accepted

If you have connected to iLO but it does not accept your login name and password, you must verify that your login information is configured correctly. Have a user who has the Administer User Accounts privilege log in and change your password. If you are still unable to connect, have the user log in again and delete and re-add your user account.

**NOTE:** The RBSU can also be used to correct login problems.

## Inability to Access the Login Page

If you cannot access the login page, you must verify the SSL encryption level of your browser and iLO. The browser and iLO encryption levels must be consistent.

HP recommends that you use the 128-bit high encryption pack.

## Inability to Access iLO Using Telnet

If you cannot access iLO using Telnet, you must verify the Remote Console Port Configuration and Remote Console Data Encryption on the **Global Settings** screen. If Remote Console Port Configuration is set to **Automatic**, the Remote Console applet enables port 23, starts a session, and then closes port 23 when the session is completed. Telnet cannot automatically enable port 23, so it fails. For more information on Telnet settings, refer to the "Telnet Support (on page 83)" section.

## Proxy Server Issues

If the Web browser software is configured to use a proxy server, it will not connect to the iLO IP address. To resolve this issue, configure the browser not to use the proxy server for the IP address of iLO. For example, in Internet Explorer, select **Tools, Internet Options, Connections, LAN Settings, Advanced**, and then enter the iLO IP address or DNS name in the **Exceptions** field.

## Firewall Issues

iLO communicates through several configurable TCP/IP ports. If these ports are blocked, the administrator must configure the firewall to allow for communications on these ports. Refer to the **Global Settings** option in the **Administration** tab to view or change port configurations.

## Inability to Access Virtual Media or Graphical Remote Console

Virtual media and graphical Remote Console are only enabled by licensing the optional iLO Advanced Pack. A message is displayed to inform the user that the features are not available without a license. Although up to 10 users are allowed to log into iLO, only one user can access the remote console. A warning message is displayed to say that the Remote Console is already in use.

## Resetting Integrated Lights-Out

In rare instances, it might be necessary to reset iLO; for example, if iLO is not responding to the browser. To reset iLO, you must power down the server and disconnect the power supplies completely.

iLO may reset itself in certain instances. For example, an internal iLO watchdog timer resets if the firmware detects an iLO problem. If a firmware upgrade is completed or a network setting is changed, iLO also resets.

The HP Management Agents 5.40 and later have the ability to reset iLO. To reset iLO, use the **Reset iLO** option on the HP Management Agent Web page under the iLO section.

You can also manually force the iLO management processor to reset by clicking **Apply** on the **Network Settings** page. You do not need to change any parameters before clicking **Apply**.

## Troubleshooting Video and Monitor Problems

The following sections discuss items to be aware of when attempting to resolve video and monitor issues.

## General Guidelines

- The client screen resolution must be greater than the screen resolution of the remote server.
- The iLO Remote Console only supports the ATI Rage XL video chip that is integrated in the system. The Remote Console functionality of iLO does not work if you install a plug-in video card. All other iLO functionality is available if you choose to use a plug-in video card.
- Only one user at a time is allowed to access the Remote Console. Check to see if another user is logged into iLO.

## Inability to Navigate the Single Cursor of the Remote Console to Corners of the Remote Console Window

In some cases, you may be unable to navigate the mouse cursor to the corners of the Remote Console window. If so, right-click and drag the mouse cursor outside the Remote Console window and back inside.

If the mouse still fails to operate correctly, or if this situation occurs frequently, verify that your mouse settings match those recommended in the "Optimizing Performance for Graphical Remote Console (on page 16)" section.

## Remote Console Text Window not Updating Properly

When using the Remote Console to display text windows that scroll at a high rate of speed, the text window might not update properly. This error is caused by video updates occurring quicker than the iLO firmware can detect and display them. Typically, only the upper left corner of the text window updates while the rest of the text window remains static. After the scrolling is complete, click **Refresh** to properly update the text window.

One known example of this issue is during the Linux booting and posting process, in which some of the POST messages can be lost. A possible repercussion is that a keyboard response will be requested by the boot process and will be missed. To avoid this issue, the booting and posting process should be slowed down by editing the Linux startup script to allow more time for keyboard responses.

## Telnet Displays Incorrectly in DOS

When using the iLO Telnet session to display text screens involving a maximized DOS window, the telnet session is unable to represent anything except the upper portion of the screen if the server screen is larger than 80x25.

To correct this adjust the DOS® windows properties to limit its size to 80x25, before maximizing the DOS window.

- On the title bar of the DOS® window, right click the mouse and select **Properties** and select **Layout**.
- On the **Layout** tab, change the **Screen Buffer Size** height to 25.

## Video Applications not Displaying in the Remote Console

Some video applications, such as Microsoft® Media Player, will not display, or will display incorrectly, in the Remote Console. This problem is most often seen with applications that use video overlay registers. Typically, applications that stream video use the video overlay registers. iLO is not intended for use with this type of application.

## Troubleshooting Miscellaneous Problems

The following sections discuss troubleshooting miscellaneous hardware or software issues.

### Remote Console Mouse Control Issue

While using Remote Console on a server running Microsoft® Windows® Server 2003, mouse movement can be very slow and it might be difficult to navigate to each of the four corners of the screen. When trying to reach a far corner of the screen, the mouse can disappear completely.

**NOTE:** This mouse behavior is more pronounced when the Remote Console session is running in a browser applet window that is smaller than the size of the server screen, and scrolling is required to see the full contents of the screen, which are not displayed.

To resolve this issue, change the following settings:

1. Click **Start, Control Panel, Mouse Properties** from the Windows® Server 2003 desktop applet.
2. Disable the Enhance pointer precision parameter.

## **Emulating a PS/2 Keyboard in a Headless Server Environment**

iLO will emulate a PS/2 keyboard in a headless server environment. When iLO detects that the server is going through POST, iLO scans for a PS/2 keyboard. If no local PS/2 keyboard is detected, iLO will be the PS/2 keyboard for the server.

A consequence of only scanning for a PS/2 keyboard at server POST time is that iLO will not implement hot-plug PS/2 keyboard functionality. If a user plugs in a PS/2 keyboard after the server POST, the keyboard will not be detected and will not work. If a user unplugs the PS/2 keyboard after the server has gone through POST, but before the operating system loads, the operating system will be unable to accept keystrokes from the Remote Console. The server must be rebooted to force iLO to rescan for a PS/2 keyboard.

## **iLO RBSU Unavailable after iLO and Server Reset**

If the iLO processor is reset and the server is immediately reset, there is a small chance that the iLO firmware will not be fully initialized when the server performs its initialization and attempts to invoke the iLO RBSU. In this case, the iLO RBSU will be unavailable or the iLO Option ROM code will be skipped altogether. If this happens, reset the server a second time. To avoid this issue, wait a few seconds before resetting the server after resetting the iLO processor.

## **Inability to Connect to the iLO Processor through the NIC**

If you cannot connect to the iLO processor through the NIC, try any or all of the following troubleshooting methods:

- Confirm that the green LED indicator (link status) on the iLO RJ-45 connector is on. This indicates a good connection between the PCI NIC and the network hub.
- Look for intermittent flashes of the green LED indicator, which indicates normal network traffic.
- Run the iLO RBSU to confirm that the NIC is enabled and verify the assigned IP address and subnet mask.

- Run the iLO RBSU and use the **F1 – Advanced** tab inside of the **DNS/DHCP** page to see the status of DHCP requests.
- Ping the IP address of the NIC from a separate network workstation.
- Attempt to connect with browser software by typing the IP address of the NIC as the URL. You can see the iLO Home page from this address.
- Reset iLO.

**NOTE:** If a network connection is established, you may have to wait up to 90 seconds for the DHCP server request.

ProLiant BL p-Class servers have a diagnostic port available. Connecting a live network cable to the diagnostic port will cause iLO to automatically switch from the iLO port to the diagnostic port. When switching between the diagnostic and back ports, you must allow one minute for the network switchover to be complete before attempting connection through the Web browser.

### Inability to Connect to the iLO Diagnostic Port

If you cannot connect to the iLO Diagnostic Port through the NIC, be aware of the following:

- The use of the diagnostic port is automatically sensed when an active network cable is plugged into it. When switching between the diagnostic and back ports, you must allow one minute for the network switchover to be complete before attempting connection through the Web browser.
- If a critical activity is in progress, the diagnostic port cannot be used until the critical activity is complete. Critical activities include:
  - Firmware upgrade
  - Remote Console session
  - SSL initialization
- If you are using a client workstation that contains more than one enabled NIC, such as a wireless card and a network card, a routing issue may prevent you from accessing the diagnostic port. To resolve this issue:
  1. Have only one active NIC on the client workstation. For example, disable the wireless network card.

2. Configure the IP address of the client workstation network to match the iLO Diagnostic Port network.
  - a. The IP address setting should be 192.168.1.X, where X is any number other than 1, because the IP address of the diagnostic port is set at 192.168.1.1.
  - b. The subnet mask setting should be 255.255.255.0.

### **Inability to Get SNMP Information from Insight Manager 7**

The agents running on the managed server supply SNMP information to Insight Manager 7. For agents to pass information through iLO, the iLO device drivers must be installed. Refer to the "Installing iLO Device Drivers" section for installation instructions.

If you have installed the drivers and agents for iLO, verify that iLO and the management PC are on the same subnet. You can verify this quickly by pinging iLO from the management PC. See your network administrator for proper routes to access the network interface of iLO.

### **Inability to Connect to iLO after Changing Network Settings**

Verify that both sides of the connection, the NIC and the switch, have the same settings for transceiver speed autoselect, speed, and duplex. For example, if one side is autoselecting the connection, then the other side should as well. The settings for the iLO NIC are controlled in the **Network Settings** screen.

### **Incorrect Time or Date of the Entries in the Event Log**

You can update the time and date on iLO by running the RBSU. This utility automatically sets the time and date on the processor using the server time and date. The time and date are also updated by Insight Management agents on supported network operating systems.

### **Inability to Upgrade iLO Firmware**

If you attempt to upgrade the iLO firmware and it does not respond, does not accept the firmware upgrade, or is terminated before a successful upgrade, the following options are available:



- iLO network flash recovery
- ROMPaq

### **iLO Network Flash Recovery**

The iLO network flash recovery payload enables you to recover from a failed firmware upgrade. The flash recovery payload uses FTP, which can only be used when the flash recovery payload is active, to transfer the firmware image to iLO. The flash recovery payload should only be used if:

- Previous firmware upgrade attempts have failed.
- You are unable to connect to the Web browser.
- There is no other firmware upgrade option available. Servers with a floppy drive can use the ROMPaq option. ProLiant BL p-Class servers must use the flash recovery payload.

If the iLO firmware image is damaged, missing, or otherwise corrupted, then the iLO flash recovery process is used to re-flash iLO. The flash recovery process is for the sole purpose of getting the system re-flashed. No other processes can be run until the recovery process is complete.

### **Diagnostic Steps**

Before attempting a flash recovery of the firmware, use the following diagnostic steps to verify that flash recovery is needed:

1. Attempt to connect to iLO through the Web browser. If you are unable to connect, then there is a communication problem.
2. Attempt to ping iLO. If you are successful, then the network is working.
3. Attempt to open an FTP session to the IP address or DNS name of iLO. If you are successful, then the flash recovery payload is active and it is necessary to upgrade the firmware using the flash recovery process.
4. If you cannot open an FTP session, then the system is not in recovery mode. Attempt to reset iLO using the steps in the "Resetting iLO ("Resetting Integrated Lights-Out" on page 234)" section.

### Flash Recovery Process

If you have verified that the flash recovery process is necessary through the diagnostic steps:

1. Open an FTP session to the IP address or DNS name of iLO.
2. Log in to iLO using a fixed user name of flash and a password of recovery. The user name and password are case sensitive.
3. At the FTP prompt, enter the put command and the file name of the firmware image.

The following is an example of the entries used for the flash recovery process:

```
ftp 192.168.177.142
login: flash
password: recovery
put \iLO140.bin
```

- If the file is found, then the put command transfers the file to iLO, the image is validated, and the flashing process begins.
- If the file is not found, then some versions of the put command will not report an error message.
- If the directory path includes spaces, enclose the path and file name in quotes.

After the firmware image is transferred, the recovery payload calculates the checksum, validates the digital signature, and reports if the image is valid. The flash reprogramming begins if the image is valid and flashing progress is then reported to the client.

**NOTE:** This process will take a few seconds while the recovery payload decrypts the stored hash and computes a hash for the image to compare against. If the image is valid, the FTP server begins programming the image into the flash part and providing status updates.

When completed, the flash recovery payload module disconnects and reboots the iLO processor. If the flash recovery process is unsuccessful, attempt the process again, while you view the progress for any errors. It might be necessary to use a different firmware image for the process.

## ROMPaq

Using ROMPaq to upgrade the iLO firmware involves two procedures: The first can be performed on any computer, and the second must be performed on the iLO host server.

1. Complete this procedure on any computer:
  - a. Download the latest iLO firmware SoftPaq. Select the SoftPaq image for diskettes and save it to the hard drive. The SoftPaq can be downloaded at HP website (<http://www.hp.com/servers/lights-out>).
  - b. Execute the SoftPaq to create diskettes.
2. Complete this procedure only on the iLO host server:
  - a. Boot the system from the ROMPaq diskette.
  - b. From the A:\ prompt, enter  
rompaq
  - c. Press the **Enter** key at the ROMPaq welcome screen. A screen displays the devices in your computer that can be upgraded.
  - d. Use the cursors to select **iLO Management** and press the **Enter** key. A screen displays the firmware images that ROMPaq can install.
  - e. Use the cursors to highlight the appropriate image and press the **Enter** key.
  - f. Press the **Enter** key again. ROMPaq reads the firmware image. If you are prompted to enter additional diskettes because you copied files to more than one diskette, put in the appropriate diskette and press the **Enter** key.
  - g. Press the **Enter** key again to begin reprogramming the ROM. Do not power cycle, reboot, or turn off the system while this process is taking place.
  - h. After you receive a message that the flash programming has completed successfully, press the **Enter** key.
  - i. Press the **Enter** key to reprogram another device, or press the **Esc** key to return to the A:\ prompt.

**NOTE:** It might be necessary to set the Security Override Switch to perform the ROMPaq upgrade. The ROMPaq program informs you if the Security Override Switch needs to be set.

## iLO Management Port not Accessible by Name

The iLO Management Port can use either a WINS server or a Dynamic DNS (DDNS) server to provide the name-to-IP address resolution necessary to access the iLO Management Port by name. The WINS or DDNS server must be up and running before the iLO Management Port is powered on, and the iLO Management Port must have a valid route to the WINS or DDNS server.

In addition, the iLO Management Port must be configured with the IP address of the WINS or DDNS server. Use DHCP to configure the DHCP server with the necessary IP addresses. You can also enter the IP addresses through RBSU or the **Network Settings** option on the **Administration** tab.

The iLO Management Port must be configured to register with either a WINS server or a DDNS server. These options are turned on as factory defaults and can be changed through RBSU or the **Network Settings** option on the **Administration** tab.

The clients used to access the iLO Management Port must be configured to use either the same WINS server with which the iLO Management Port was registered, or the same DDNS server where the IP address of the iLO Management Port was registered.

If you are using a WINS server and a nondynamic DNS server, the access to the iLO Management Port may be significantly faster if you configure the DNS server to use the WINS server for name resolution. Refer to the appropriate Microsoft® documentation for more information.

## Event Log Entries

Event Log Display	Event Log Explanation
Server power failed	Displays when the server power fails.
Browser login: <i>IP address</i>	Displays the IP address for the browser that logged in.
Server power restored	Displays when the server power is restored.
Browser logout: <i>IP address</i>	Displays the IP address for the browser that logged out.
Server reset	Displays when the server is reset.
Failed Browser login – IP Address: <i>IP address</i>	Displays when a browser login fails.
iLO Self Test Error: #	Displays when iLO has failed an internal test. The probable cause is that a critical component has failed. Further use of iLO on this server is not recommended.
iLO reset	Displays when iLO is reset.
On-board clock set; was #:#:#:#:#	Displays when the onboard clock is set.
Server logged critical error(s)	Displays when the server logs critical errors.
Event log cleared by: <i>User</i>	Displays when a user clears the event log.
iLO reset to factory defaults	Displays when iLO is reset to the default settings.
iLO ROM upgrade to #	Displays when the ROM has been upgraded.
iLO reset for ROM upgrade	Displays when iLO is reset for the ROM upgrade.
iLO reset by user diagnostics	Displays when iLO is reset by user diagnostics.
Power restored to iLO	Displays when the power is restored to iLO.
iLO reset by watchdog	Displays when an error has occurred in iLO and iLO has reset itself. If this problem persists, call customer support.
iLO reset by host	Displays when the server resets iLO.
Recoverable iLO error, code #	Displays when a non-critical error has occurred in iLO and iLO has reset itself. If this problem persists, call customer support.
SNMP trap delivery failure: <i>IP address</i>	Displays when the SNMP trap does not connect to the specified IP address.

<b>Event Log Display</b>	<b>Event Log Explanation</b>
Test SNMP trap alert failed for: <i>IP address</i>	Displays when the SNMP trap does not connect to the specified IP address.
Power outage SNMP trap alert failed for: <i>IP address</i>	Displays when the SNMP trap does not connect to the specified IP address.
Server reset SNMP trap alert failed for: <i>IP address</i>	Displays when the SNMP trap does not connect to the specified IP address.
Illegal login SNMP trap alert failed for: <i>IP address</i>	Displays when the SNMP trap does not connect to the specified IP address.
Diagnostic error SNMP trap alert failed for: <i>IP address</i>	Displays when the SNMP trap does not connect to the specified IP address.
Host generated SNMP trap alert failed for: <i>IP address</i>	Displays when the SNMP trap does not connect to the specified IP address.
Network resource shortage SNMP trap alert failed for: <i>IP address</i>	Displays when the SNMP trap does not connect to the specified IP address.
iLO network link up	Displays when the network is connected to iLO.
iLO network link down	Displays when the network is not connected to iLO.
iLO Firmware upgrade started by: <i>User</i>	Displays when a user starts a firmware upgrade.
Host server reset by: <i>User</i>	Displays when a user resets the host server.
Host server powered OFF by: <i>User</i>	Displays when a user powers off a host server.
Host server powered ON by: <i>User</i>	Displays when a user powers on a host server.
Virtual Floppy in use by: <i>User</i>	Displays when a user begins using a Virtual Floppy.
Remote Console login: <i>User</i>	Displays when a user logs on a Remote Console session.
Remote Console Closed	Displays when a Remote Console session is closed.
Failed Console login - IP Address: <i>IP address</i>	Displays a failed console login and IP address.
Added User: <i>User</i>	Displays when a local user is added.
User Deleted by: <i>User</i>	Displays when a local user is deleted.
Modified User: <i>User</i>	Displays when a local user is modified.

Event Log Display	Event Log Explanation
Browser login: <i>User</i>	Displays when a valid user logs on to iLO using an Internet browser.
Browser logout: <i>User</i>	Displays when a valid user logs off iLO using an Internet browser.
Failed Browser login – IP Address: <i>IP address</i>	Displays when a browser login attempt fails.
Remote Console login: <i>User</i>	Displays when an authorized user logs on using the Remote Console port.
Remote Console Closed	Displays when an authorized Remote Console user is logged out or when the Remote Console port is closed following a failed login attempt.
Failed Console login – IP Address: <i>IP address</i>	Displays when an unauthorized user has failed three login attempts using the Remote Console port.
Added User: <i>User</i>	Displays when a new entry is made to the authorized user list.
User Deleted by: <i>User</i>	Displays when an entry is removed from the authorized user list. The User section displays the user who requested the removal.
Event Log Cleared: <i>User</i>	Displays when the user clears the Event Log.
Power Cycle (Reset): <i>User</i>	Displays when the power has been reset.
Virtual Power Event: <i>User</i>	Displays when the Virtual Power Button is used.
Security Override Switch Setting is On	Displays when the system is booted with the Security Override Switch set to On.
Security Override Switch Setting Changed to Off	Displays when the system is booted with the Security Override Switch changed from On to Off.
On-board clock set; was previously [NOT SET]"	Displays when the on-board clock is set. Will display the previous time or "NOT SET" if there was not a time setting previously.
Logs full SNMP trap alert failed for: <i>IP address</i>	Displays when the logs are full and the SNMP trap alert failed for a specified IP address.
Security disabled SNMP trap alert failed for: <i>IP address</i>	Displays when the security has been disabled and the SNMP trap alert failed for a specified IP address.

<b>Event Log Display</b>	<b>Event Log Explanation</b>
Security enabled SNMP trap alert failed for: <i>IP address</i>	Displays when the security has been enabled and the SNMP trap alert failed for a specified IP address.
Virtual Floppy connected by <i>User</i>	Displays when an authorized user connects the Virtual Floppy.
Virtual Floppy disconnected by <i>User</i>	Displays when an authorized user disconnects the Virtual Floppy.
License added by: <i>User</i>	Displays when an authorized user adds a license.
License removed by: <i>User</i>	Displays when an authorized user removes a license.
License activation error by: <i>User</i>	Displays when there is an error activating the license.
iLO RBSU user login: <i>User</i>	Displays when an authorized user logs in to iLO RBSU.
Power on request received by: <i>Type</i>	A power request was received as one of the following types:  Power Button  Wake On LAN  Automatic Power On
Virtual NMI selected by: <i>User</i>	Displays when an authorized user selects the Virtual NMI button.
Virtual Serial Port session started by: <i>User</i>	Displays when a Virtual Serial Port session is started.
Virtual Serial Port session stopped by: <i>User</i>	Displays when a Virtual Serial Port session is ended.
Virtual Serial Port session login failure from: <i>User</i>	Displays when there is a login failure for a Virtual Serial Port session.



---

# Technical Support

## In This Section

HP Contact Information.....	249
Before You Contact HP.....	249

## HP Contact Information

For the name of the nearest HP authorized reseller:

- In the United States, call 1-800-345-1518.
- In Canada, call 1-800-263-5868.
- In other locations, refer to the HP website (<http://www.hp.com>).

For HP technical support:

- In North America, call the HP Technical Support Phone Center at 1-800-652-6672. This service is available 24 hours a day, 7 days a week. For continuous quality improvement, calls may be recorded or monitored.
- Outside North America, call the nearest HP Technical Support Phone Center. For telephone numbers for worldwide Technical Support Centers, refer to the HP website (<http://www.hp.com>).

## Before You Contact HP

Be sure to have the following information available before you call HP:

- Technical support registration number (if applicable)
- Product serial number
- Product model name and number
- Applicable error messages
- Add-on boards or hardware

- Third-party hardware or software
- Operating system type and revision level

# Acronyms and Abbreviations

**ACPI**

Advanced Configuration and Power Interface

**ARP**

Address Resolution Protocol

**ASCII**

American Standard Code for Information Interchange

**CA**

certificate authority

**CR**

Certificate Request

**DHCP**

Dynamic Host Configuration Protocol

**DNS**

Domain Name System

**EMS**

Emergency Management Services

**FEH**

fatal exception handler

**FSMO**

Flexible Single-Master Operation

**HB**

heartbeat

**ICMP**

Internet Control Message Protocol

**iLO**

Integrated Lights-Out

**IML**

Integrated Management Log

**IP**

Internet Protocol

**LDAP**

Lightweight Directory Access Protocol

**LED**

light-emitting diode

**LOM**

Lights-Out Management

**MMC**

Microsoft® Management Console

**NIC**

network interface controller

**NVRAM**

non-volatile memory

**POST**

Power-On Self-Test

**PSP**

ProLiant Support Pack

**RAS**

remote access service

**RBSU**

ROM-Based Setup Utility

**RIBCL**

Remote Insight Board Command Language

**RILOE**

Remote Insight Lights-Out Edition

**RILOE II**

Remote Insight Lights-Out Edition II

**SNMP**

Simple Network Management Protocol

**SSL**

Secure Sockets Layer

**UID**

unit identification

**USB**

universal serial bus

**VM**

Virtual Machine

**VPN**

virtual private networking

**XML**

extensible markup language

# Index

## A

activation 225  
 Active Directory 105  
 ADD\_USER 157, 165  
 additional information 249  
 administration 63, 65, 68, 72, 74, 76, 77, 141, 142, 212  
 alert and trap problems 228  
 alerts 87  
 authorized reseller 249

## B

batch processing 145  
 BL p-Class 77, 223  
 Browser-Based Setup 15

## C

CLEAR\_EVENTLOG 192  
 commands 150, 163, 164, 165, 168, 169, 171, 173, 175, 176, 177, 179, 183, 185, 186, 188, 189, 190, 192, 194, 195, 197, 198, 199, 200, 201, 202, 203, 204, 205  
 configuration options 13, 14, 15, 18  
 connection overview 29, 30  
 CPQLODOS 150, 152  
 cursor modes 27

## D

data protection methods 88  
 data types 159  
 DELETE\_USER 168  
 device drivers, installing 19, 20, 21  
 Device Queries 143  
 Directory Services 99, 101, 105, 122, 219  
 Directory Services for eDirectory 122

Directory Services Objects 113, 128  
 directory services settings 155  
 Directory settings 135, 219, 220

## E

eDirectory 122  
 enabling 99  
 error messages 159

## F

features 99

## G

GET\_ALL\_USERS 173  
 GET\_DIR\_CONFIG 185  
 GET\_FIRMWARE\_VERSION 194  
 GET\_GLOBAL\_SETTINGS 188  
 GET\_HOST\_POWER\_STATUS 202  
 GET\_NETWORK\_SETTINGS 177  
 GET\_TOPOLOGY 200  
 GET\_UID\_STATUS 205  
 GET\_USER 169  
 global settings 68, 214

## H

hardware troubleshooting 231  
 HOTKEY\_CONFIG 195

## I

iLO Advanced Functionality 15, 18, 50  
 Insight Manager 7 85, 87, 88, 221  
 Insight Manager 7 integration 89

## L

LDAP 122  
 LEDs 229  
 LICENSE 197  
 Lights-Out DOS Utility 149

Lights-Out Management 121, 134  
LOGIN 163

## **M**

MOD\_BLADE\_RACK 199  
MOD\_DIR\_CONFIG 155, 186, 187  
MOD\_GLOBAL\_SETTINGS 189  
MOD\_NETWORK\_SETTINGS 152  
MOD\_SNMP\_IM\_SETTINGS 190

## **N**

NetWare server support 21  
network settings 65, 216

## **O**

operational overview 30, 85, 149, 160  
optimizing performance 16  
overview, RIBCL 160

## **P**

port matching 87  
preparation procedures 101, 105, 122

## **Q**

queries 143  
query definition 143

## **R**

RACK\_INFO 198  
Remote Console 46, 49  
required information 249  
required software 101, 227  
RESET\_RIB 177  
RESET\_SERVER 204  
RIB\_INFO 176  
RIBCL 159, 160  
ROM-Based Setup Utility (RBSU) 14

## **S**

schema documentation 99  
schema installer 101  
scripts 160  
server identification 211  
SERVER\_INFO 201  
SET\_HOST\_POWER 203  
settings 17, 18, 77, 99  
Snap-In installer 104  
SNMP alerts 15  
software troubleshooting 231  
supported software 25, 26, 100  
system status 40, 41, 42, 43

## **T**

technical support 249  
telephone numbers 249  
Telnet 83

## **U**

UID\_CONTROL 205  
UPDATE\_RIB\_FIRMWARE 193  
usage model 28  
user access 35, 39, 40, 138  
USER\_INFO 164  
using virtual media 55

## **V**

virtual devices 50, 51, 53, 55, 61, 62  
virtual indicators 62  
Virtual Media 53, 55, 58, 59, 60  
Virtual Power button 51  
Virtual Serial port 61

## **W**

Windows server support 20

## **X**

XML header 161



XML, general guidelines 160